WELCOME

SSH Capital Markets Day 2025

SSH CMD 2025 Agenda

Opening words

Henri Österlund, Chairman of the Board

Where to play and how to win

Rami Raulas, CEO

From Secure Protocols to Holistic Public Safety

Miikka Sainio, CTO

15-minute break

Integrating AI Across SSH's Operations and Solutions

Jussi Löppönen, Principal Engineer, AI

Beyond Quantum Confusion

Suvi Lampila, SSH Fellow

Tero Mononen, Principal Engineer, Cryptography and Protocols

SSH and Leonardo (video)

Simone Ungaro, Co-General Manager, Strategy & Innovation

Financial update

Michael Kommonen, CFO

Q&A

SSH

Opening words

Henri Österlund
Chairman of the Board, SSH
Founding Partner, Accendo Capital

Capital Markets Day

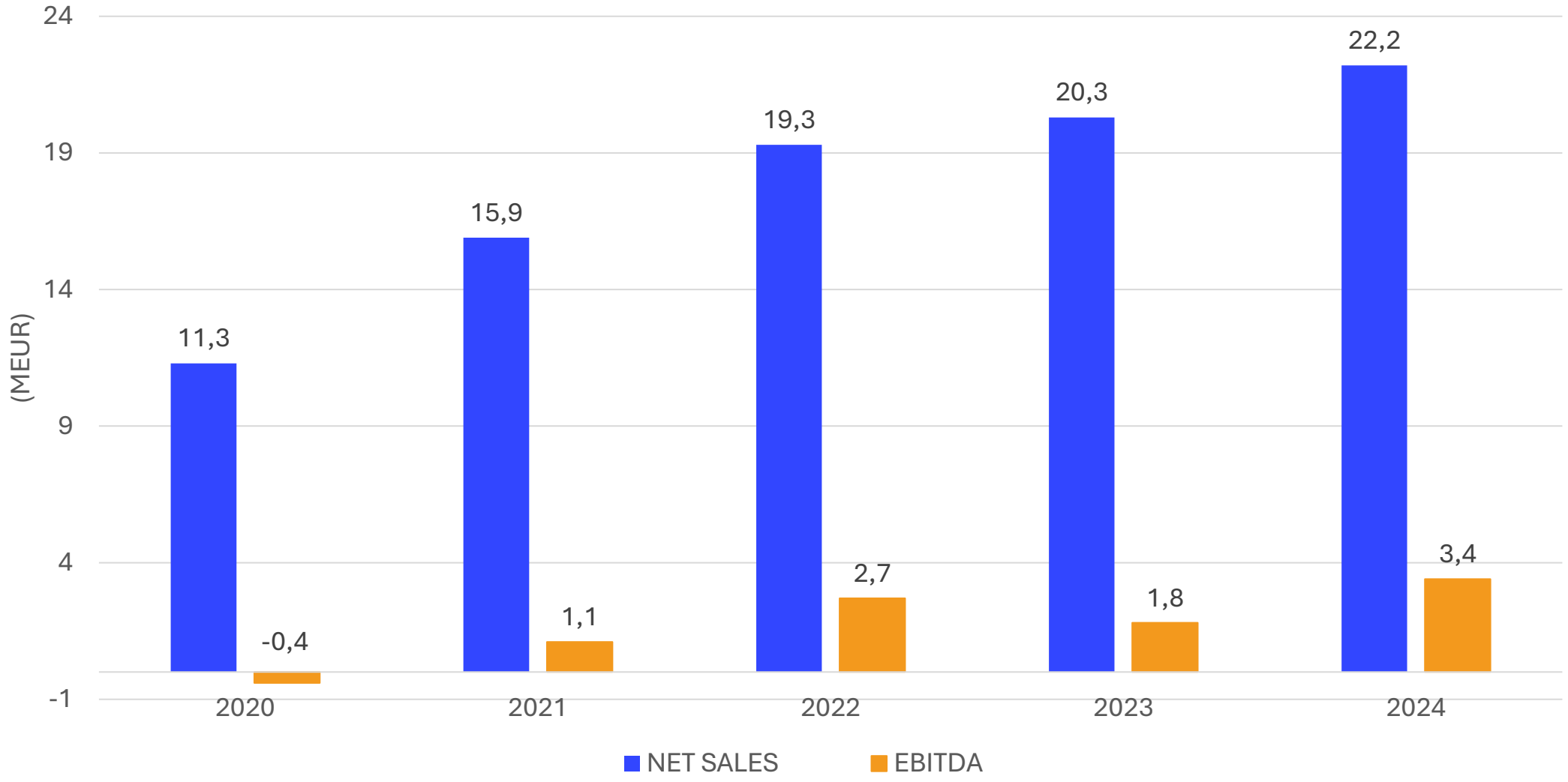
Where to Play, How to Win

Rami Raulas, CEO

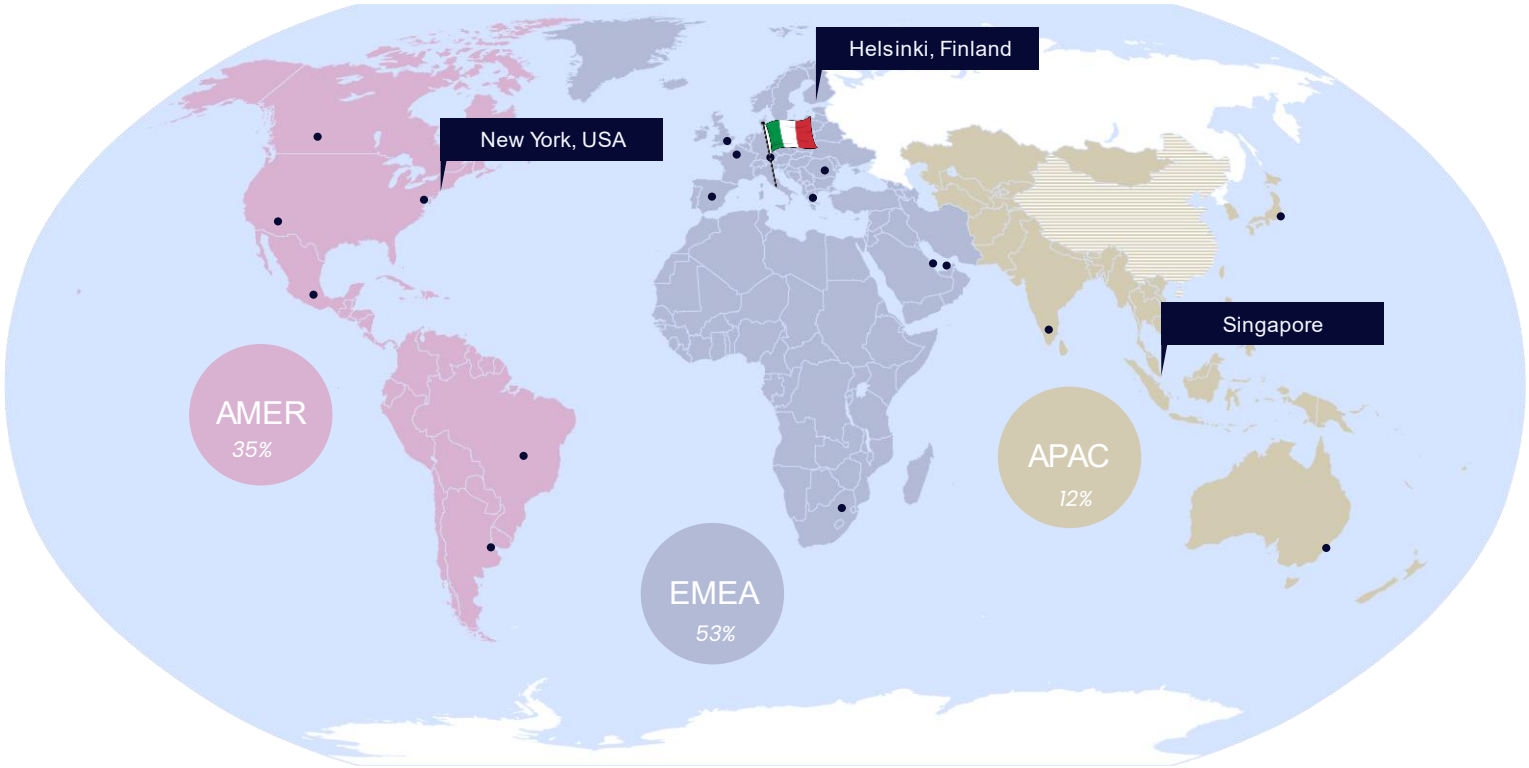
Oct 23, 2025

SSH

Net sales and EBITDA 2020-2024



SSH Communications Security



SSH Communications Security

Competitive portfolio, integrated

Renewed

SSH

Where to Play

Trends, challenges, regulation, risks
= Demand

Market segments

Solution Domains

How to Win

Solutions
&
Services & **S**upport

Marketing -> demand

Sales
-> Partners
= more feet on the ground

Where to Play

Trends, challenges,
regulation, risks
= Demand

Market
segments

Solution
Domains

How to Win

Solutions
&
Services & **S**upport

Marketing -> demand

Sales
-> Partners
= more feet on the ground

SSH for Industry verticals - heritage

BANKING & FINANCE

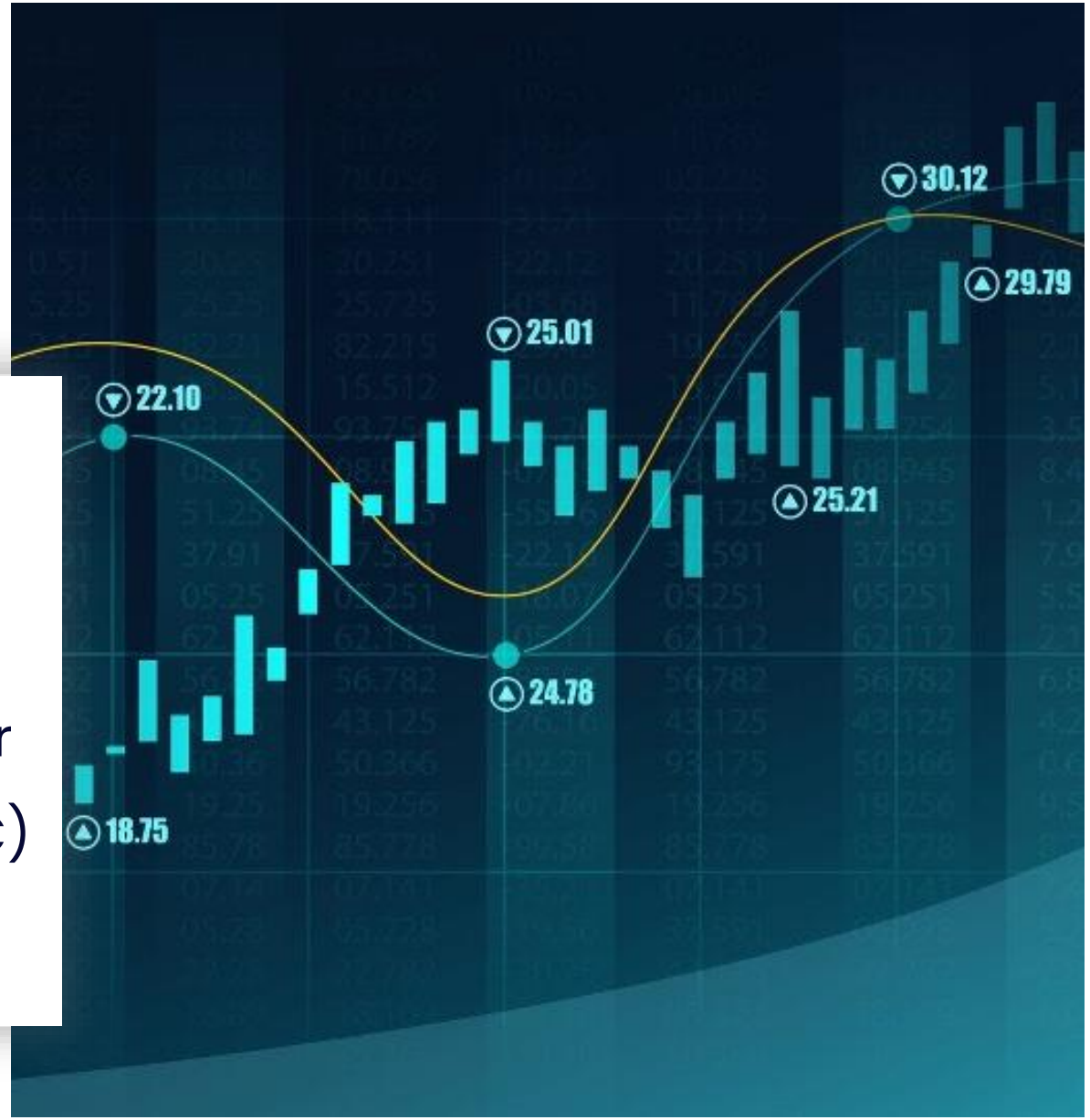
Key management solves audit problem

Major global bank

1.5 million keys renewed annually by application owners.

FINANCIAL SERVICES

Secure access for CI/CD pipelines and config management



Global Quant Trading

Modern PAM provides fine-grained secure access, session recording for High-Performance Computing (HPC) environment.

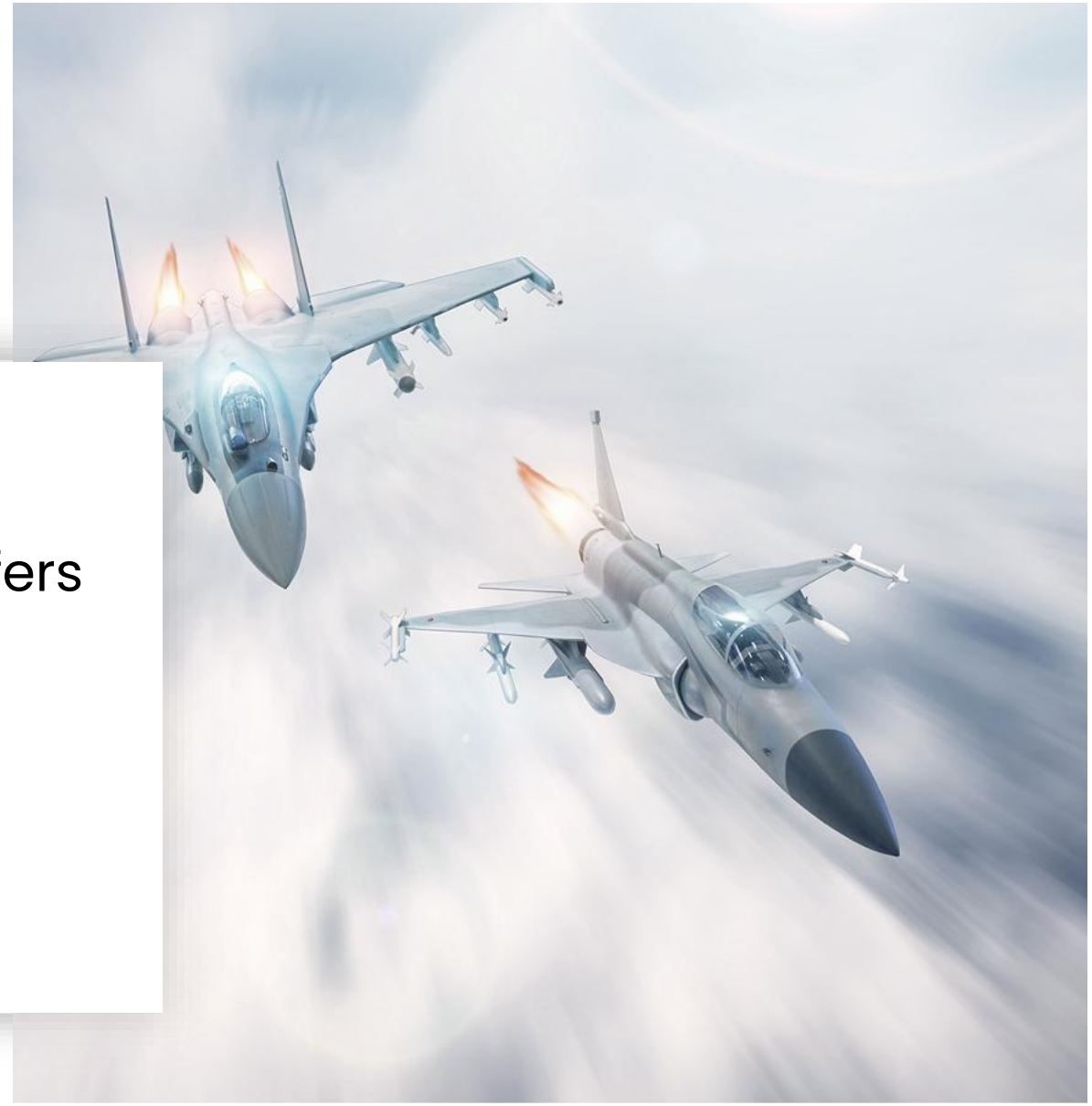
SSH


IT,
Technology,
MSP
Retail
logistics
Health Care
Finance
Insurance

New growth opportunities

SSH

Defensive Cybersecurity



- Post-Quantum Encryption
- File Encryption & Secure Data Transfers
- Secure Messaging
- Network Encryption
- Zero Trust Access Management

Approved supplier for NATO's NCI Agency

LEONARDO

CRITICAL INFRASTRUCTURES & LARGE ENTERPRISE – MARKET SEGMENTS

RAILWAY
National & Regional Railway, Metro

SMART CITY & MOBILITY
Safe Cities, Intelligent Urban Mobility

TRANSPORTATION
Railways, Metro, Tram, eBUS

ROAD INFRASTRUCTURES
MIT/ANSFISA, Roads, Bridges and Works of Art

PORTS & LOGISTICS
MIT/RAM, Ports, Interports , ZES/ZLS, Navy

NEW **AIRPORTS**
Airports, National Aviation Authority (ENAC, ENAV)

LARGE COMPANIES
General Contractors, Companies,

ENERGY INFRASTRUCTURES
Production and distribution

HYDROGEN PLANTS NEW
Large production and distribution plants

WIND OFFSHORE PLANTS NEW
Large production and distribution plants

OIL&GAS & INDUSTRY
Off-Shore, On-Shore, Pipeline, LNG

WATER/UNDERWATER NEW
Aqueducts, Dams, Wastewater, Pipelines, Cables

NUCLEAR NEW
Decommissioning, New Power Plants

BANKING
Banks, Poste

LEONARDO

Most attacked market is OT Manufacturing –
Leonardo data

Top 10 Sectors Ransomware	.. August.
Manufacturing	43
Construction	24
Consulting & Professional Services	19
Legal	19
Information Technology	17
Financial Services	15
Education	14
Food and Beverage	13
Healthcare	13
Industrial	13

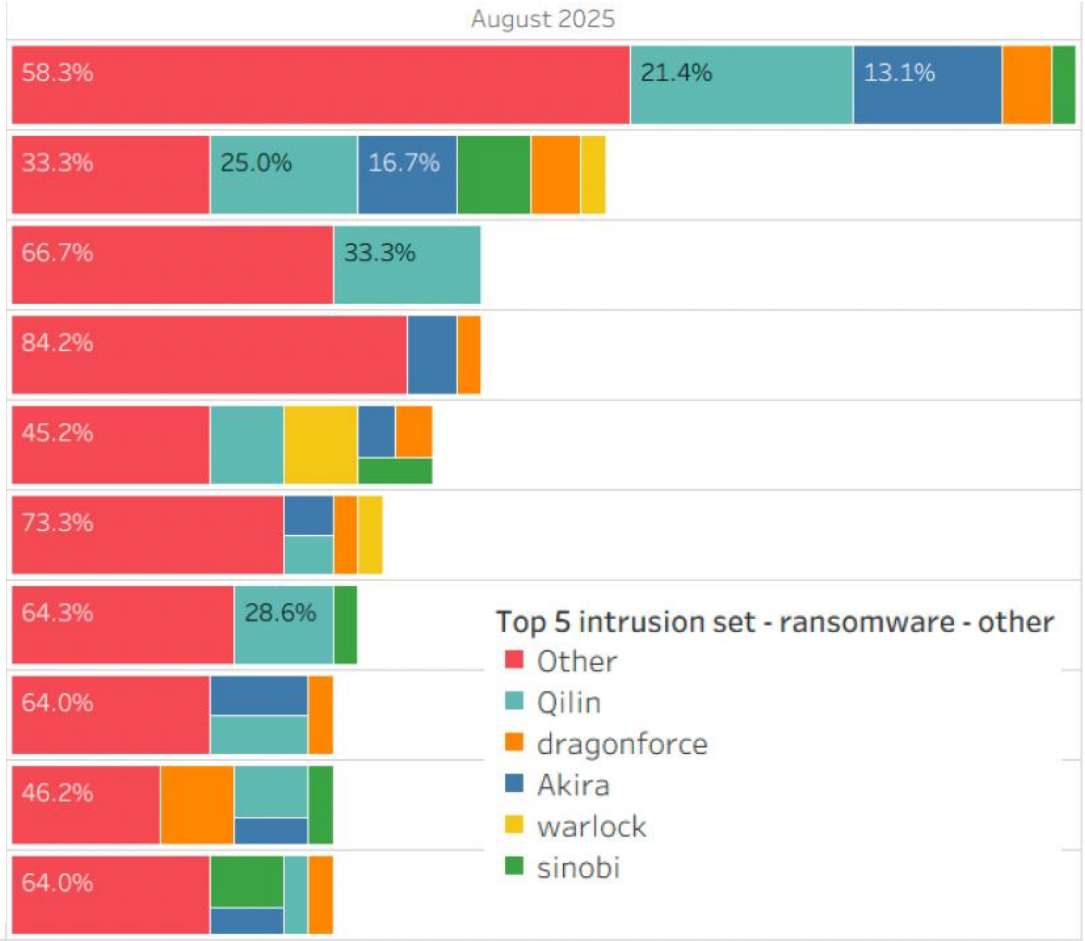


Figure 21 - Distinct count of ransomware claims broken down by top 5 Threat Actor against top 10 targeted sectors during the last month.

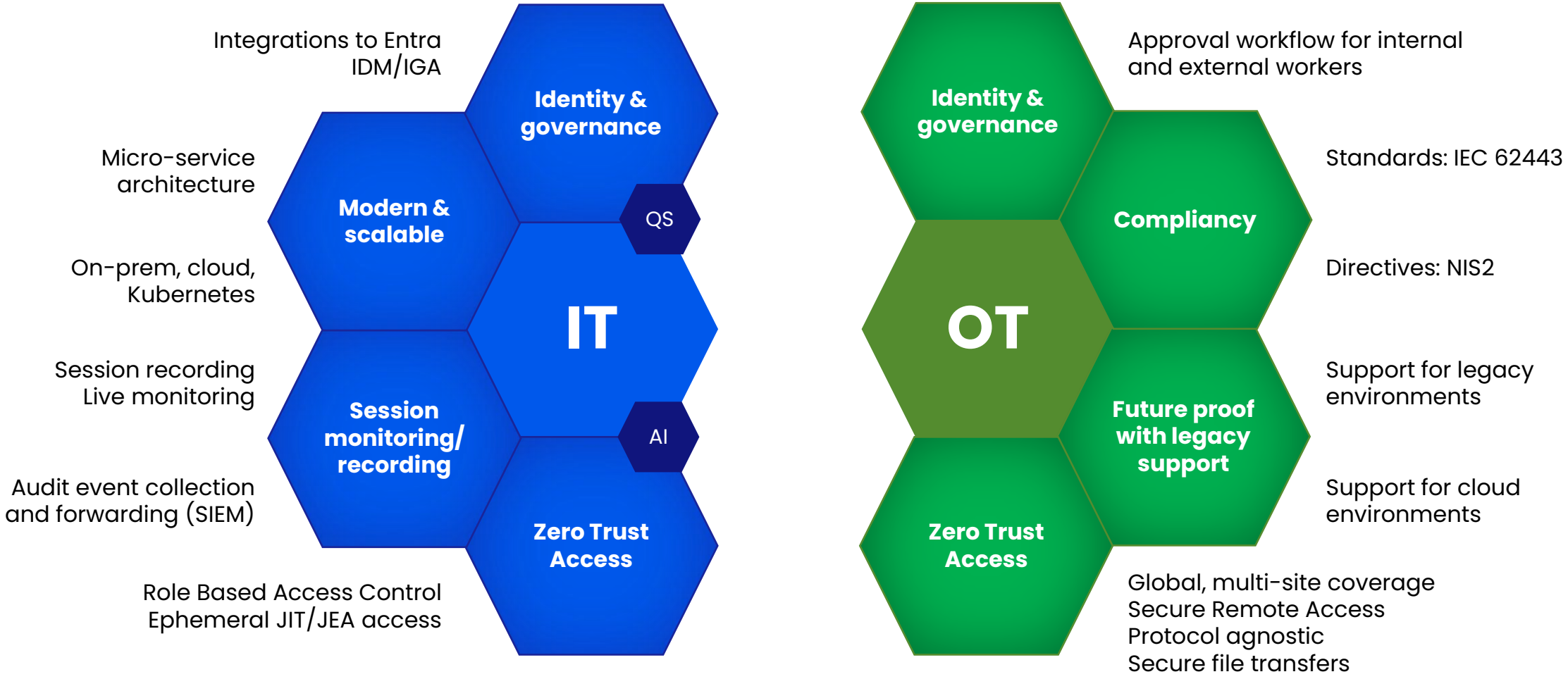
Manufacturing OT attacks cost a lot

System Shock: A Crisis in Manufacturing

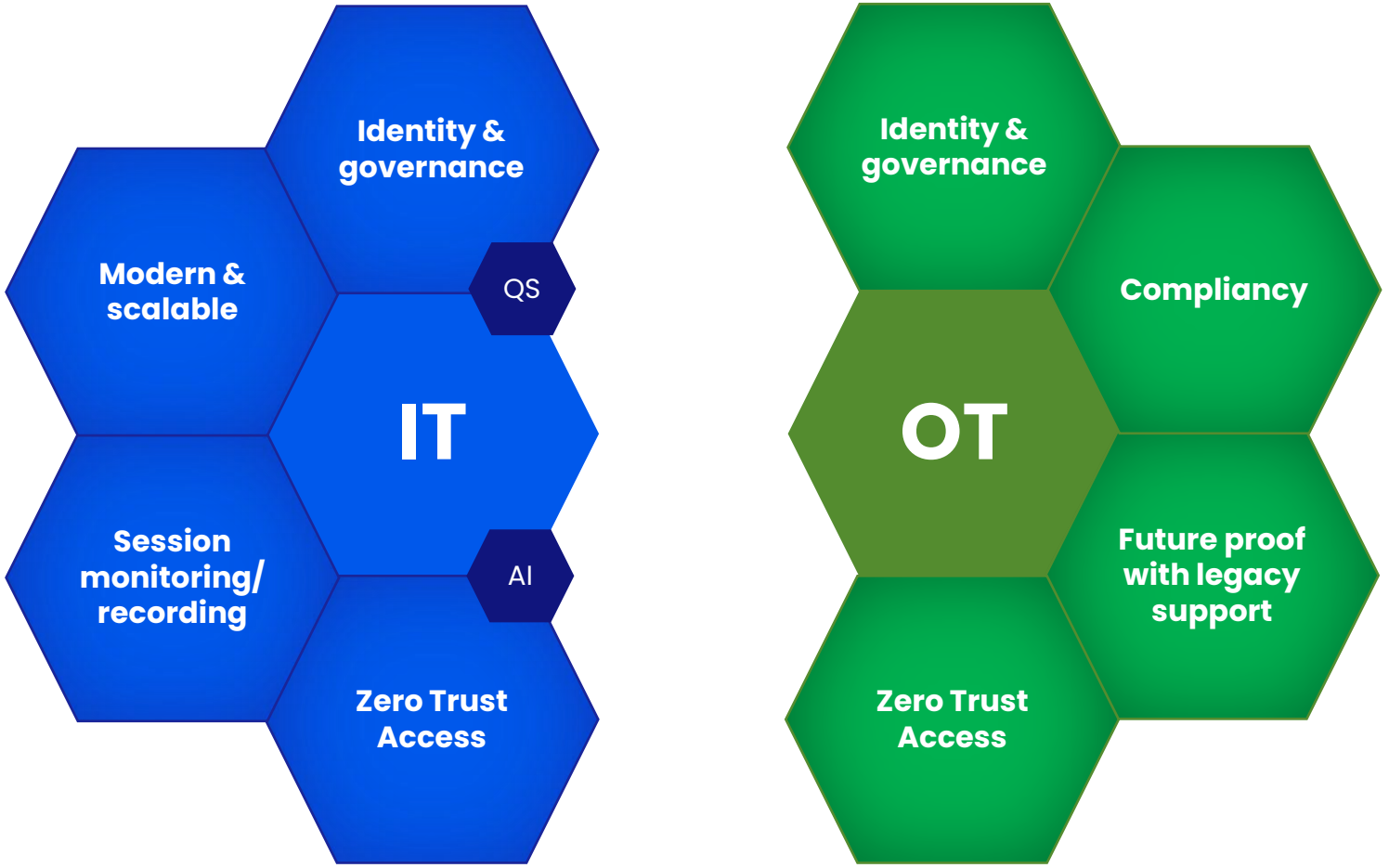
A (not so hypothetical) Global Incident in High-Value Goods

36 days Full Shutdown	**1,000+** Finished Units/Day Lost	**5** Global Manufacturing Sites Affected
£72M+ Lost Sales *per day*	**33,000** Domestic Employees Affected	**200,000** Supply Chain Jobs Impacted

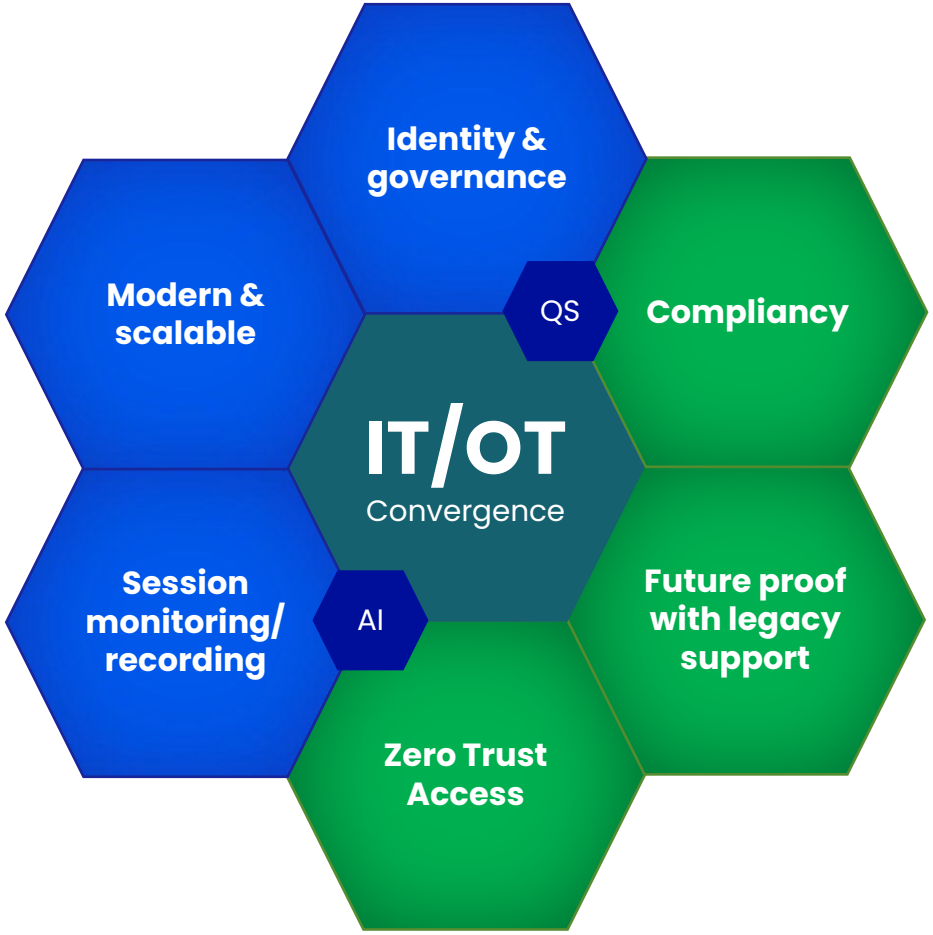
Convergence of IT and OT – Access Management



Convergence of IT and OT – Access Management



Convergence of IT and OT – Access Management




NEW

Secure Remote Access for OT/ICS Leadership Compass

kuppingercole ANALYSTS

PrivX

- Granular access control and microsegmentation
- Agentless access to legacy OT systems
- Flexible deployment options including Kubernetes and air-gapped environments

October 15th 2025

SSH

E-COMMERCE AND LOGISTICS

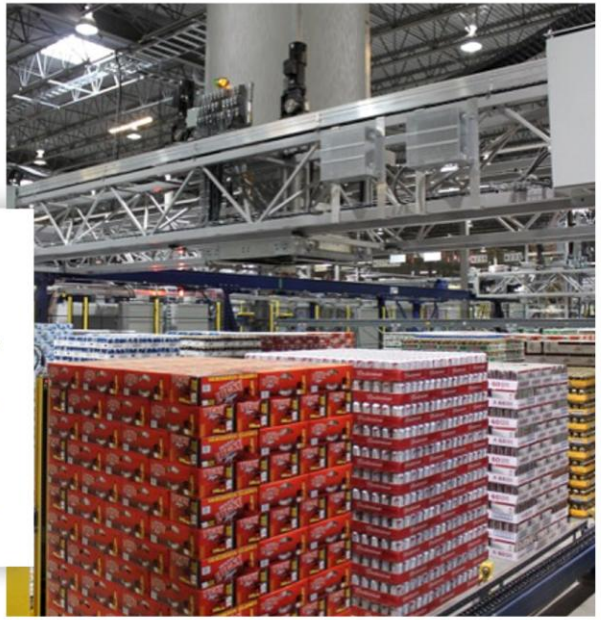
Securing robotics and control systems.

E-commerce

Securing access to robotic systems for food & beverage, grocery, retail, e-commerce, postal services and electric-vehicle battery production.

E-COMMERCE AND LOGISTICS

Securing robotics and control systems.



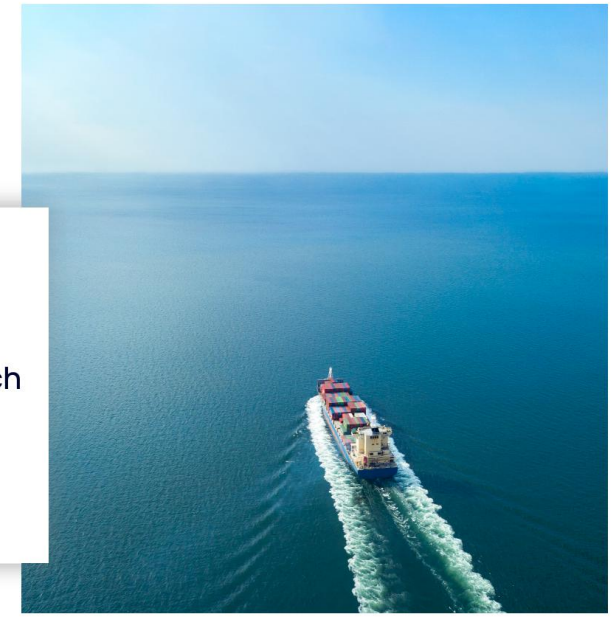
E-commerce

Securing access to robotic systems for food & beverage, grocery, retail, e-commerce, postal services and electric-vehicle battery production.

SSH

SHIPPING & MARITIME

Securing Remote Access for 1000s of ships



Marine Vessel Operator

No need to wait for the ship to reach the harbor for Diagnostics and Maintenance.

SSH

PULP & PAPER

Securing 50 sites, 10 countries, 3000 technicians and 5000 devices

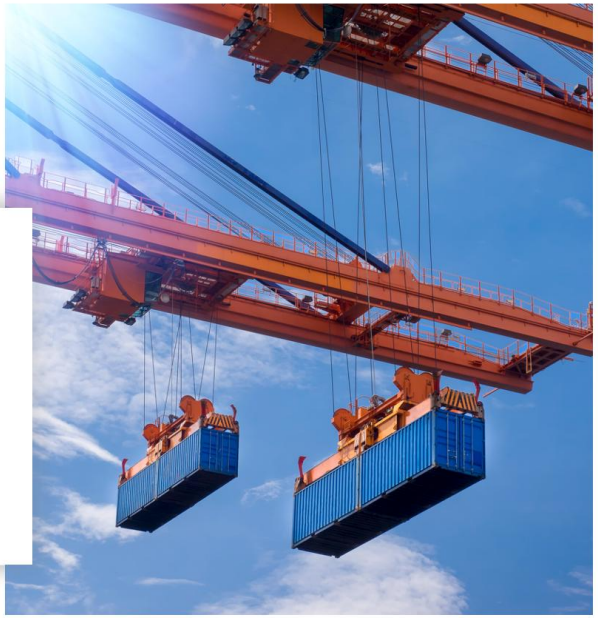
Global forest industry business

Centralized secure remote access management for technicians to multiple sites.

SSH

SHIPPING & MARITIME

Simplified, Secured Port Maintenance



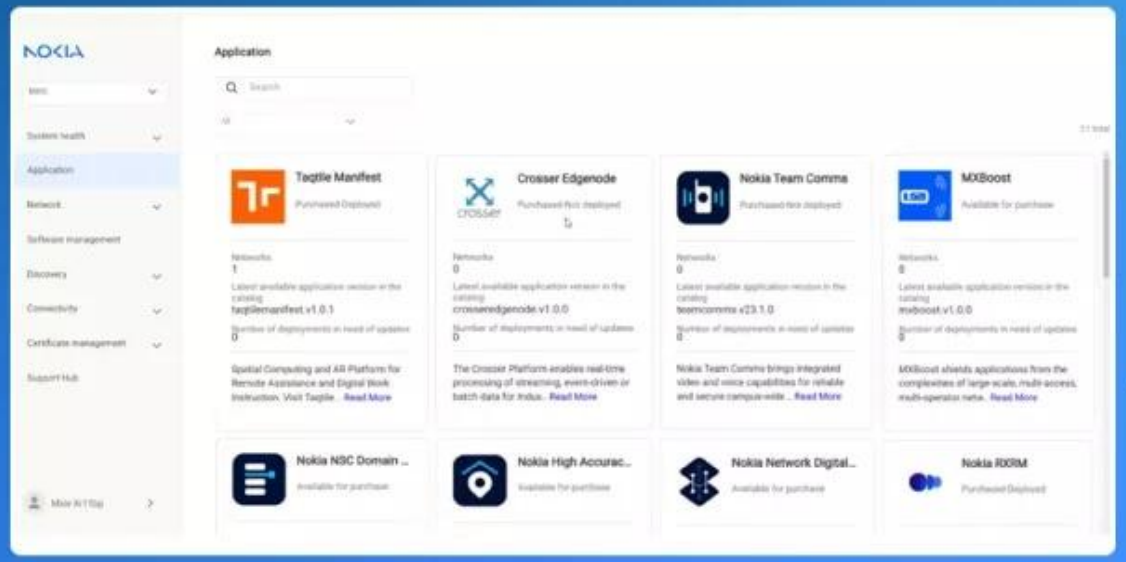
Industrial Crane Manufacturer

Just-in-Time and Just-Enough access for identified maintainers.

SSH


NEW

PrivX OT @Nokia 5G MXIE Industrial Edge MarketPlace



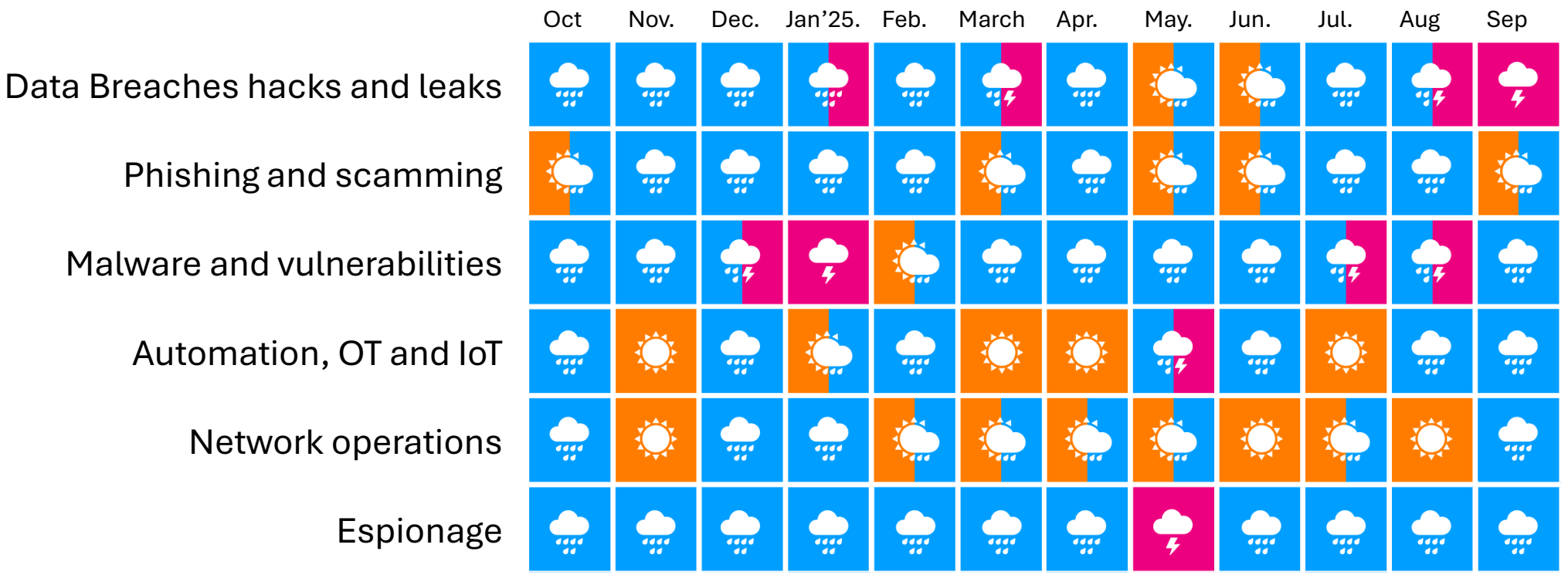
Nokia DAC MXIE manager

SSH

Trends

Market Drivers

Trends for Cybersecurity



Trends for Cybersecurity

- DDoS
- Ransomware
- State-sponsored attacks on Public Administration and Critical Infrastructures (NIS2)

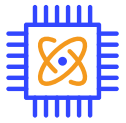
Renewed

solution portfolio

SSH

Key solution trends chosen by SSH to focus on

Quantum-Safe



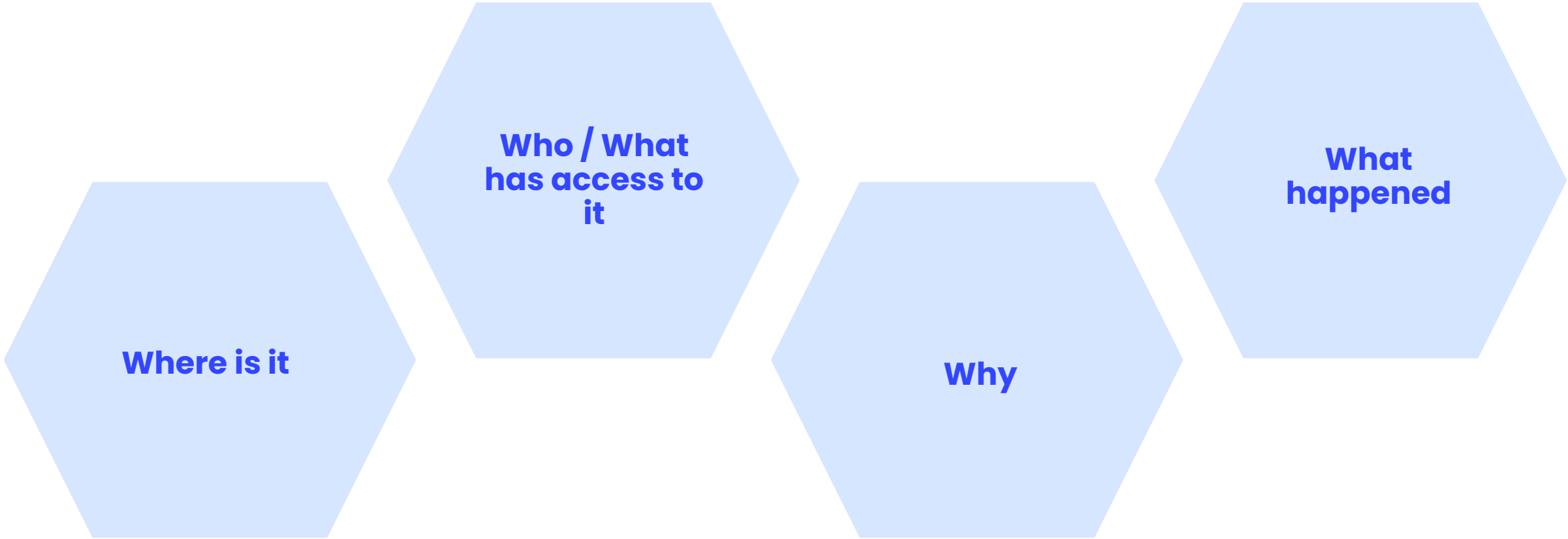
Zero Trust

AI

To whom and why

What data/systems/communications is:

- **Secret**
- **Confidential**
- **Restricted**



SSH

SSH Communications Security

Competitive portfolio, integrated

SSH Communications Security

Competitive portfolio – Quantum Safe

- Mandate to transition to Quantum-Safe (CER, EU RM, NIST…)
- Traditional Routing & Firewall Networks and Encryption Networks separate (Defence, NIST CSfC, Finance DC’s)
- Easy migration to Quantum-Safe connections (no rip&replace)
  - Easy and Safe deployments
  - Crypto-Agility
- High performance

Press release

SSH Communications Security (SSH) Announces a New Order for the NQX Quantum Safe Encryption Solution from a European Defence Organization

Helsinki, Finland – July 8, 2025. SSH Communications Security (SSH) announces a new subscription, and services order valued approximately 160,000 EUR for its NQX encryption solution, delivered to a European defence organization. NQX provides quantum-safe encryption to protect customers’ sensitive data.

The customer valued the encryption performance of NQX nodes, as well as the compact size to meet specific site requirements. In addition, the capability to utilize PQC algorithms ensures the environment is always secure and ready to withstand quantum threats. NQX has National Certification for Confidential Level and is in the process for NATO and EU certifications for 2025.

“NQX’s unique combination of uncompromising security and high-performance stems from the rigorous demands of the defence sector. As a future-proof, crypto-agile solution, NQX provides customers with the flexibility to adopt the latest quantum-safe encryption algorithms as they emerge and seamlessly integrate classical and quantum-safe encryption side-by-side, all without requiring massive hardware investments,” states Rami Raulas, CEO of SSH.

DATA CENTERS

Secure, high-bandwidth transmissions for customer data

High-performance data center provider

Quantum-safe, high bandwidth and low latency transmissions to secure managed private cloud customer data.

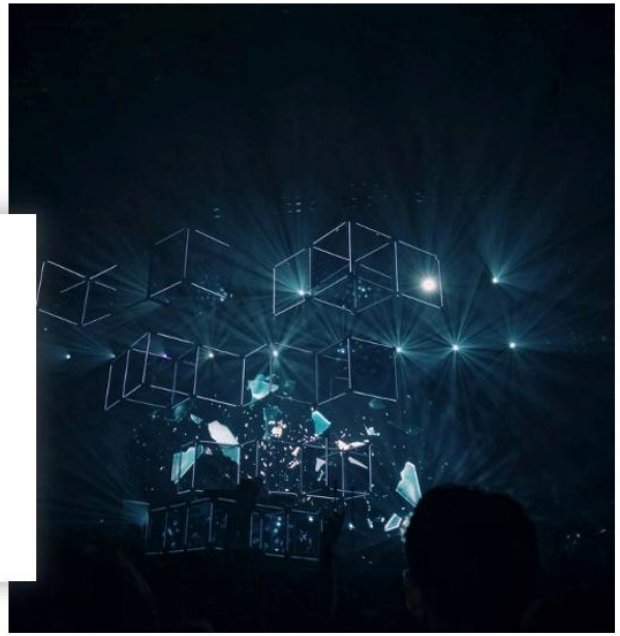
SSH

Secure, high-bandwidth transmissions for customer data

High-performance data center provider

Quantum-safe, high bandwidth and low latency transmissions

Securing data center connections across the whole estate

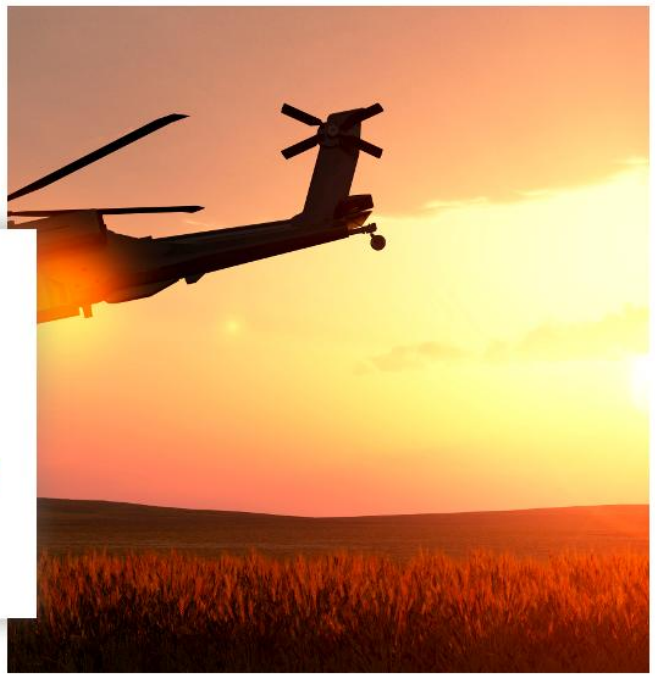


Multi-site enterprise

Mesh network. Quantum-safe encryption at the network level and transparent to users or resources communicating

SSH

Quantum-safe protection for classified data-in-transit



Critical public organization

Connecting branch offices to share classified and confidential information securely.

SSH

Quantum-safe transmission of threat intelligence

Software consultancy

Threat intelligence service and consultancy company share threat, diagnostics and assessment intelligence securely

SSH

SSH Communications Security

Competitive portfolio –sensitive data

- Secure FORMS – ROOMS - SIGN
- Secure MAIL *(“TurvaViesti”)*
- Secure MESSAGING

- Data classification, policies

- Governance

- Use Cases
  - Government
  - Defence
  - Critical Infrastucture
  - Healthcare
  - Finance & Insurance
  - Legal

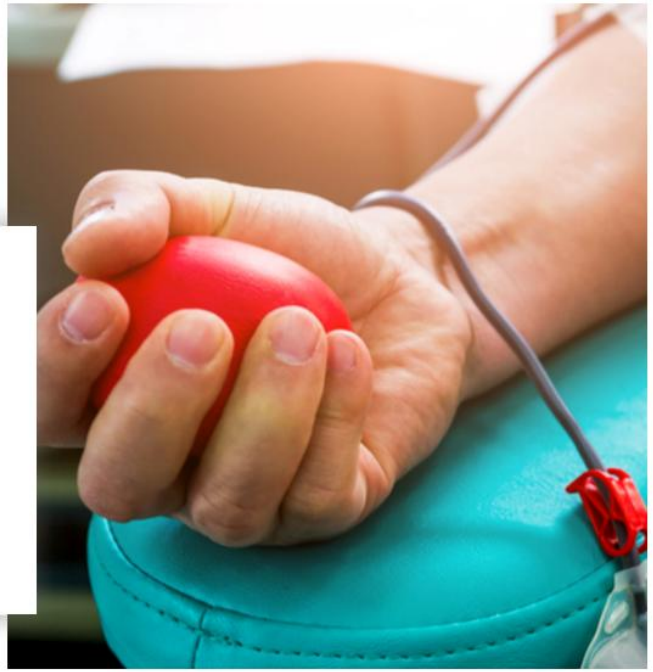
GOVERNMENT

Securing court and criminal documents

Court

Securely receive sensitive information from the public and share confidential records between authorities.

Handling health data securely



Blood service

Collect, sign, share and store sensitive health information

Securing HR information

Financial institution

Share and collect employment related information securely

SSH

Protecting sensitive financial data sharing

Financial institution

Share sensitive information (account statements, investments, etc.) with customers

SSH

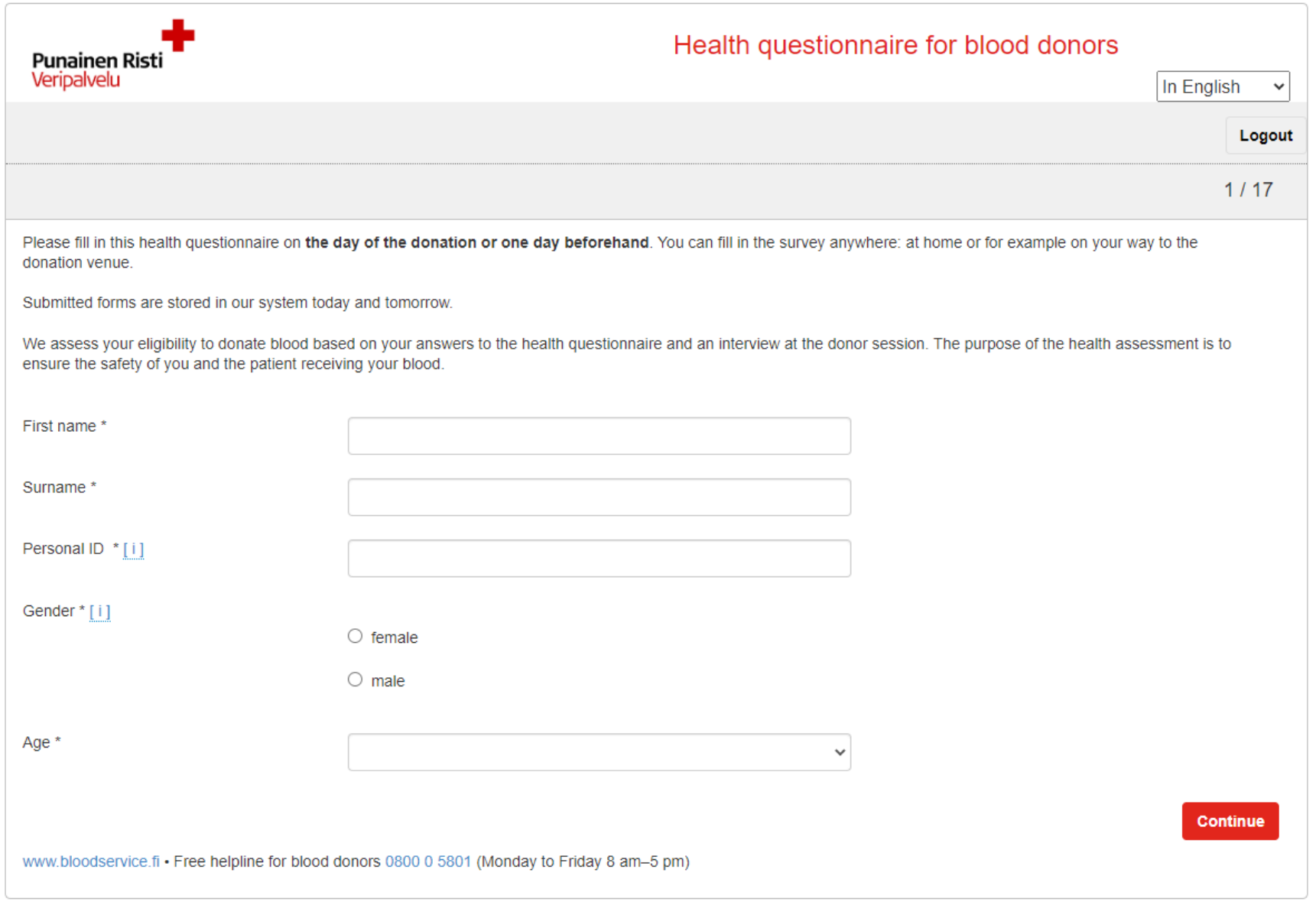
Secure communication for patients, authorities, and insurers

Healthcare provider

Secure communications integrated with identity infrastructure and the joiners-movers-leavers process

SSH

SecureFORMS



FINNISH GOVERNMENT

Encrypted message
- Send message

From your e-mail address

Continue

Processing of personal data when sending a secure email message

Before you can send a secure email message, the receiving authority must register your email address in the shared secure email service of the administrative branch of the Ministry of Justice. After the registration, you will receive a personal link to your email address, which will direct you to a protected environment for sending your secure email. Your message will not be sent from your own email nor will you receive the reply from the authority in your own email; instead, all communication takes place in a protected environment. The messages you receive in your email only contain links to a protected environment: a link for sending secure email messages, and a link to received secure email messages.

Secure email messages are individual messages that are removed from the service within 30 days. The secure email service does not have a separate mailbox for secure mail. **If you think you may need the secure email message or attachment file that you have received later, save it by clicking on the Save button at the bottom of the page, or take photographs.**

The purpose of the secure email service is to enable secure communication between the customer and the authorities. Your email address will be stored in the shared secure email service of the administrative branch of the Ministry of Justice for 30 days from the date on which your address was registered. When your email address is registered, the IP address of your device will also be stored in the information system's log. The communication log data are stored separately and used only to enable the provision of the secure email service and to investigate any disruptions and information security incidents as provided in the Act on Electronic Communication Services.

The processing of personal data in connection with the use of the secure email service is necessary in order for the controller to comply with its legal obligations (Article 32 of the EU General Data Protection Regulation, section 31 of the Act on the Processing of Personal Data in Criminal Matters and in Connection with Maintaining National Security, section 5 of the Act on the Provision of Digital Services). The technical services are provided by the Government ICT Centre (Valtori) and its contractual partner Erillisverkot Group, which is a wholly state-owned company.

For more detailed information on the processing of personal data in connection with the secure email service, please contact the authority to which you are sending the message. The authority in question acts as the controller responsible for the processing of your personal data. Contact details for the authority and its data protection officer are available on the authority's website. Everyone has the right to lodge a complaint with the Data Protection Ombudsman concerning the processing of their personal data. For more information, please see: www.tietosuoja.fi.

Accessibility-statement

Puolustusvoimat
Försvarsmakten • The Finnish Defence Forces

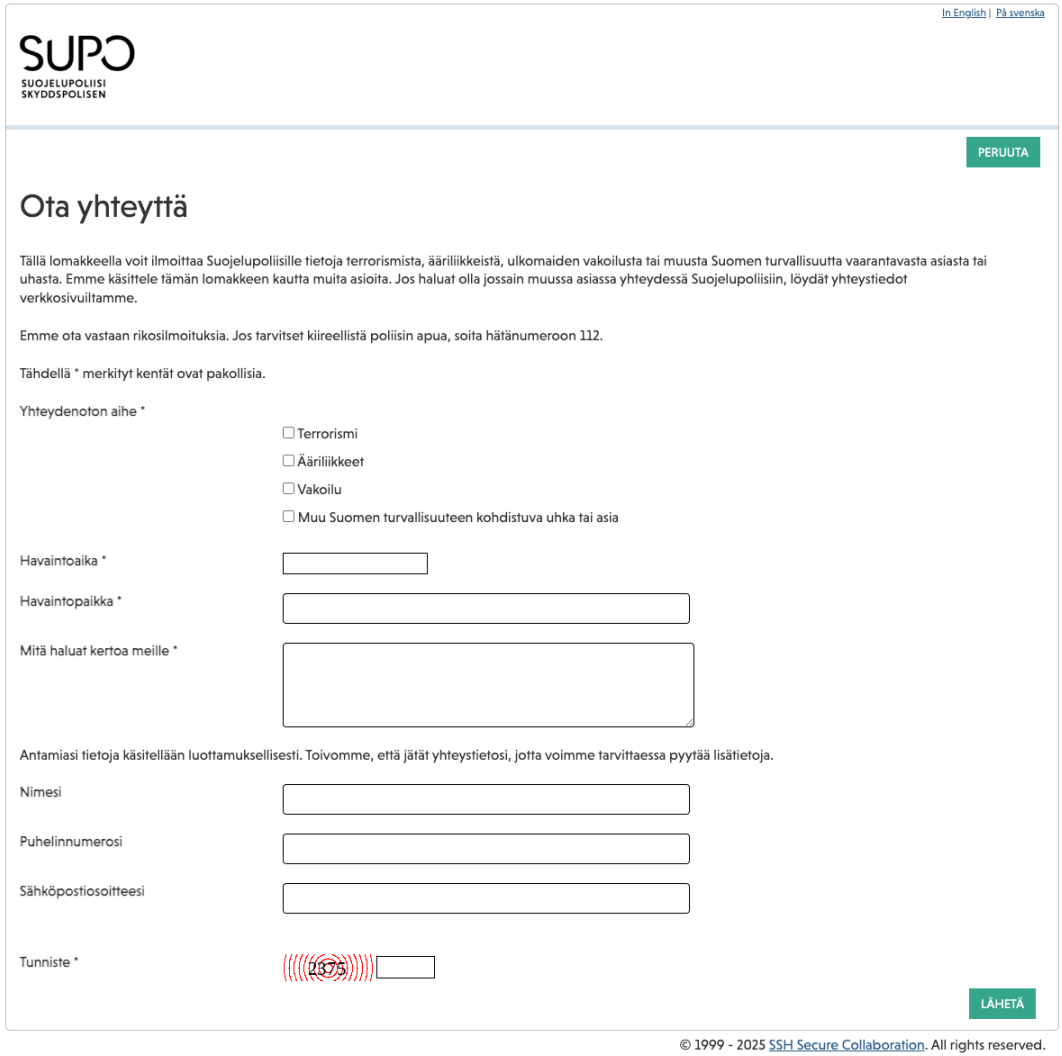
CONFIDENTIAL MESSAGE
- Send message

From your e-mail address

Continue

SSH

Secret data transmissions encrypted



In English | På svenska

SUPO
SUOJELUPOLIISI
SKYDDSPOLISEN

PERUUTA

Ota yhteyttä

Tällä lomakkeella voit ilmoittaa Suojelupoliisille tietoja terrorismista, ääriliikkeistä, ulkomaiden vakoilusta tai muusta Suomen turvallisuutta vaarantavasta asiasta tai uhasta. Emme käsittele tämän lomakkeen kautta muita asioita. Jos haluat olla jossain muussa asiassa yhteydessä Suojelupoliisiin, löydät yhteystiedot verkkosivuiltamme.

Emme ota vastaan rikosilmoituksia. Jos tarvitset kiireellistä poliisin apua, soita hätänumeroon 112.

Tähdellä * merkityt kentät ovat pakollisia.

Yhteydenoton aihe *

- ☐ Terrorismi
- ☐ Ääriliikkeet
- ☐ Vakoilu
- ☐ Muu Suomen turvallisuuteen kohdistuva uhka tai asia

Havaintoaika *

Havaintopaikka *

Mitä haluat kertoa meille *

Antamiasi tietoja käsitellään luottamuksellisesti. Toivomme, että jätät yhteystietosi, jotta voimme tarvittaessa pyytää lisätietoja.

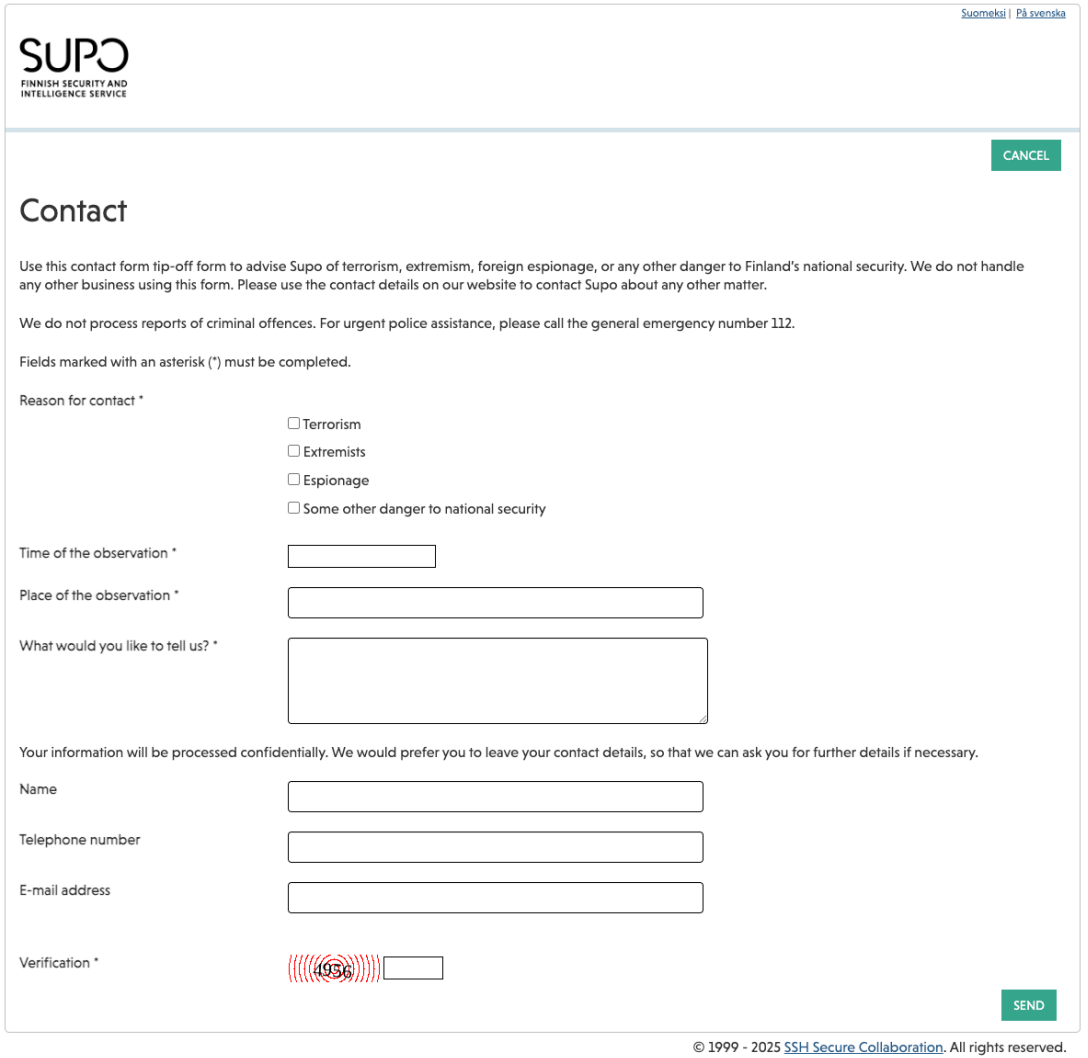
Nimesi

Puhelinnumerosi

Sähköpostiosoitteesi

Tunniste * 2375

LÄHETÄ



Suomeksi | På svenska

SUPO
FINNISH SECURITY AND INTELLIGENCE SERVICE

CANCEL

Contact

Use this contact form tip-off form to advise Supo of terrorism, extremism, foreign espionage, or any other danger to Finland's national security. We do not handle any other business using this form. Please use the contact details on our website to contact Supo about any other matter.

We do not process reports of criminal offences. For urgent police assistance, please call the general emergency number 112.

Fields marked with an asterisk (*) must be completed.

Reason for contact *

- ☐ Terrorism
- ☐ Extremists
- ☐ Espionage
- ☐ Some other danger to national security

Time of the observation *

Place of the observation *

What would you like to tell us? *

Your information will be processed confidentially. We would prefer you to leave your contact details, so that we can ask you for further details if necessary.

Name

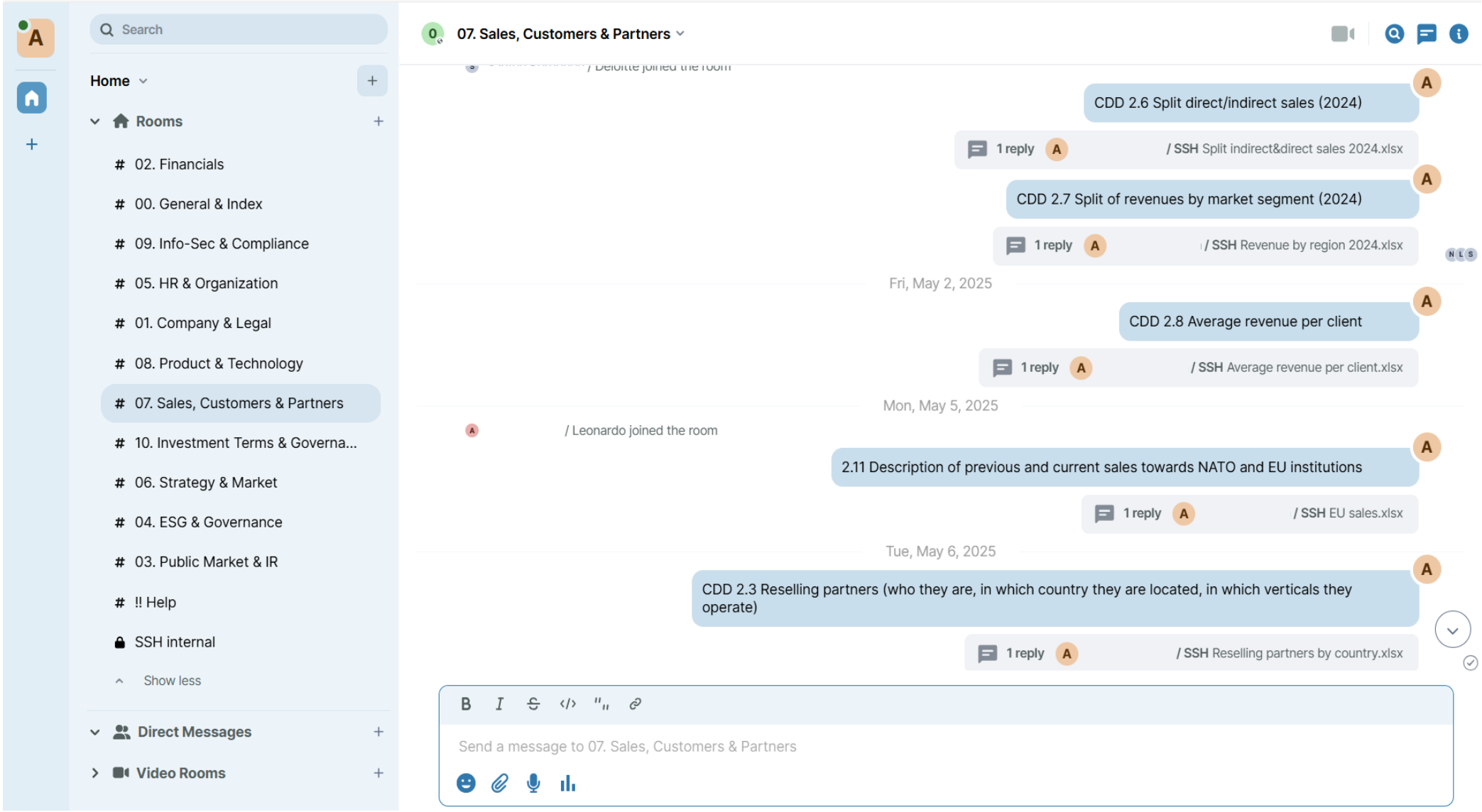
Telephone number

E-mail address

Verification * 4956

SEND

SSH SalaX for Leonardo DD



A bit of AI (order IT)

AI synthesised

AI agentic workflow

SSH IT Superstore

This is the beginning of your direct message history with **SSH IT Superstore**.
Only the two of you are in this conversation, unless either of you invites anyone to join.

Rami Raulas created this DM.

Rami Raulas invited SSH IT Superstore

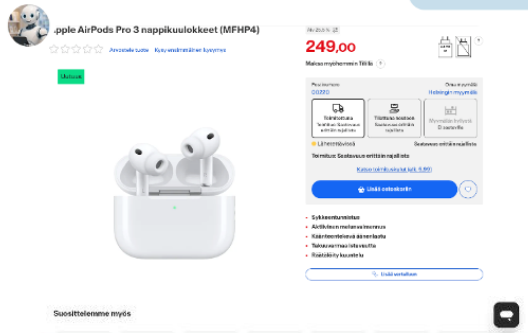
SSH IT Superstore joined the room

expand

I want to order Apple AirPods Pro 3 nappikuulokkeet (MFHP4)

Hello Rami! You are eligible for a new pair of headphones. Please provide the URL to the product link on Verkkokauppa.com.

https://www.verkkokauppa.com/fi/product/1011533/Apple-AirPods-Pro-3-nappikuulokkeet-MFHP4?utm_source=google&utm_medium=cpc&utm_campaign=Adwords%20Br%C3%A4ndit%20Apple&utm_id=1726648762&gad_source=1&gad_campaignid=1726648762&gclid=Cj0KCQjw_rPGBhCbARIsABjq9ccHDITsbDvA8e7xtbPsT2vKsYBcoSzzaO-xSXhwr_VFfQu1rW2Y6xUaAnF7EALw_wcB



Apple AirPods Pro 3 nappikuulokkeet (MFHP4)

The price for the Apple AirPods Pro 3 is €198.41. After subtracting the company part of €150, you will need to pay €48.41.

Do you approve this order?

yes

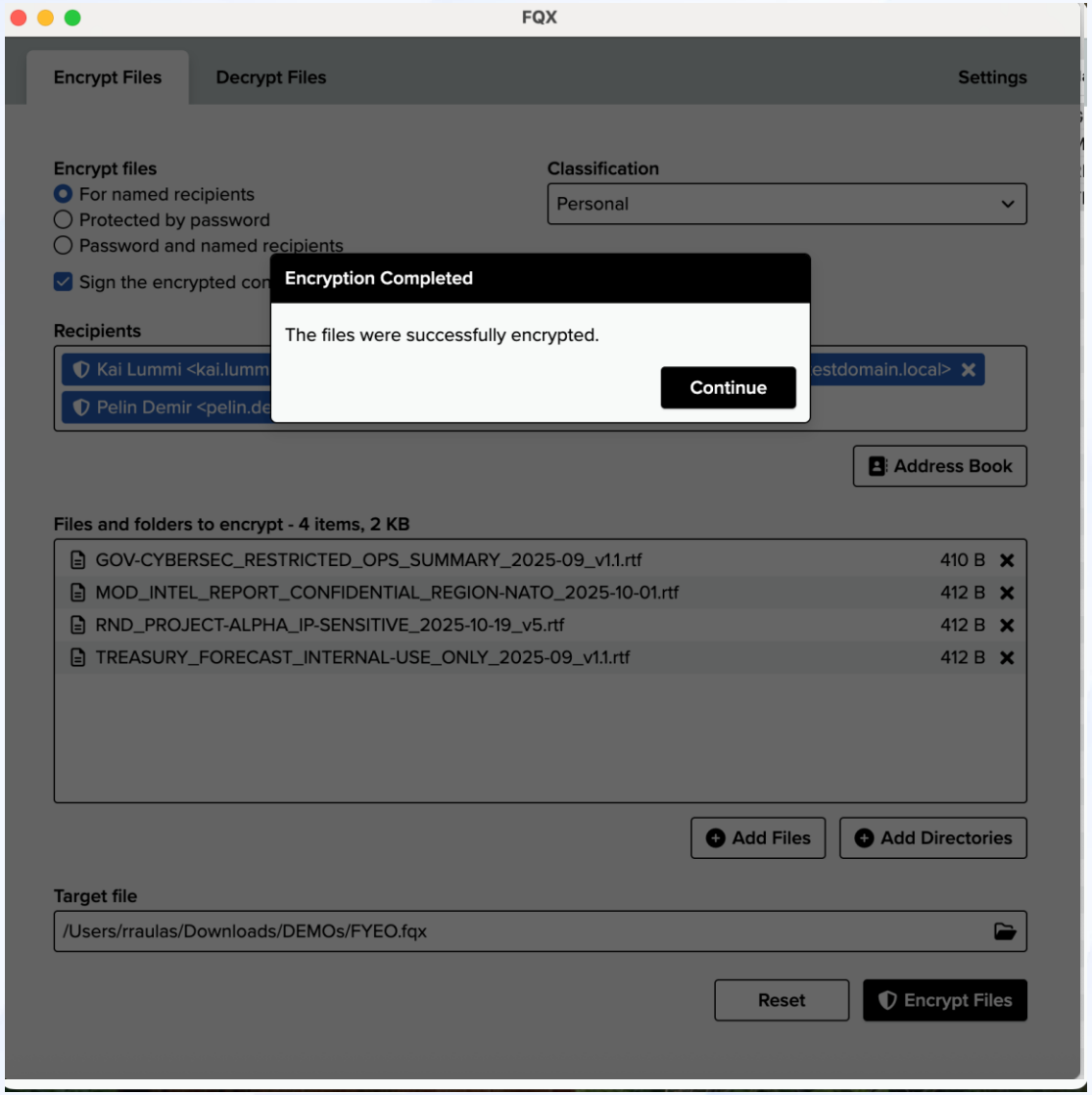
Your order for the Apple AirPods Pro 3 has been successfully placed! Thank you, Rami. If you need anything else, feel free to ask.

19:43

FQX

FYEO.fqx

- We offer multiple ways of transferring sensitive data and files securely encrypted In-Transit
  - Tectia, PrivX, SalaX
- But there is a requirement (E.g. GDPR) for encrypting data At-Rest, before sharing
- Large banks and other organizations use complicated and difficult to use PGP, and are looking for better solution
- Working on new FQX customer cases



SSH Communications Security

Competitive portfolio – Zero Trust

- PrivX is our growth engine +17 % growth in subscription sales
- Positive customer and analyst reviews and feedback

- Innovative solution
  - New generation:
  - *Just In Time*
  - *Just Enough*
  - *Strong Authentication*
  - *Ephemeral Authentication & Connections*
- Modern technology
- Secrets' Management & automation opportunity
- IT & OT
- Great ROI & TCO


NEW

GOVERNMENT

Protect access to sensitive government data

Estonia's Interior Ministry IT Centre

Centrally managed, audited and compliant access to sensitive data.

SSH

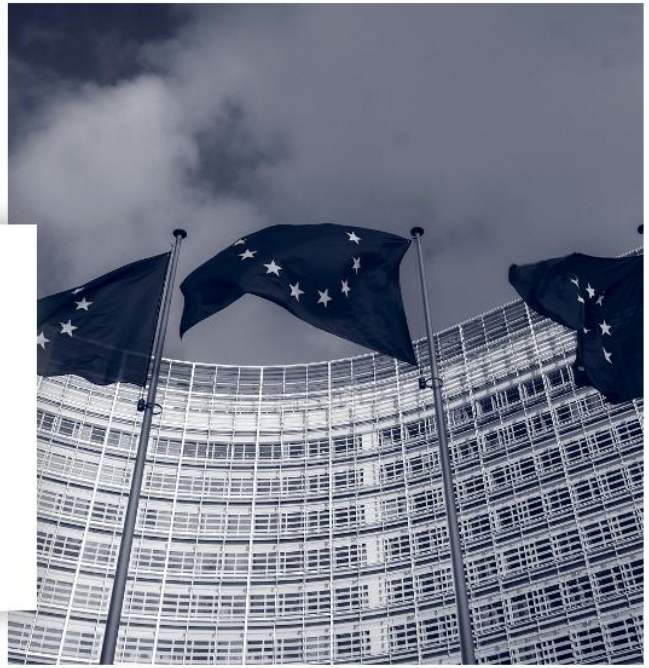
SSH

Protect access to sensitive government data

Centrally managed, audited and compliant access to sensitive data in Estonian Interior Ministry

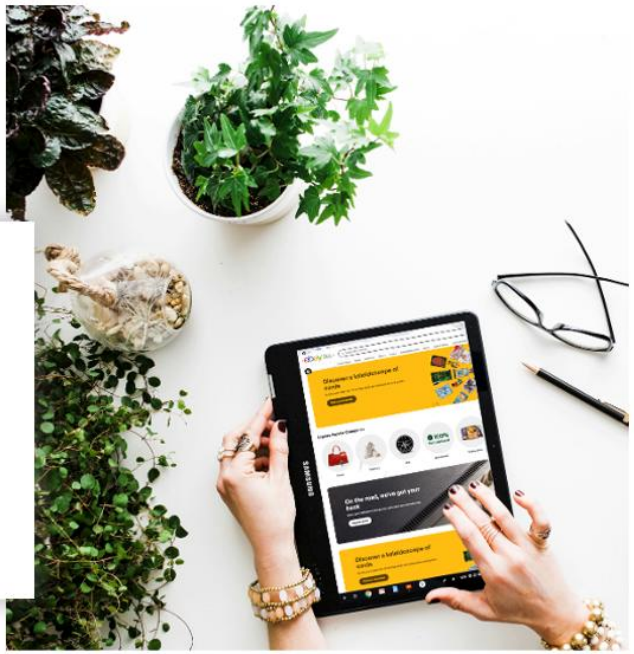
Privileged Access for 35k users in cross-regional IT environment

Large European Organization Replacing a legacy PAM for speed, simplicity and cost-efficiency.



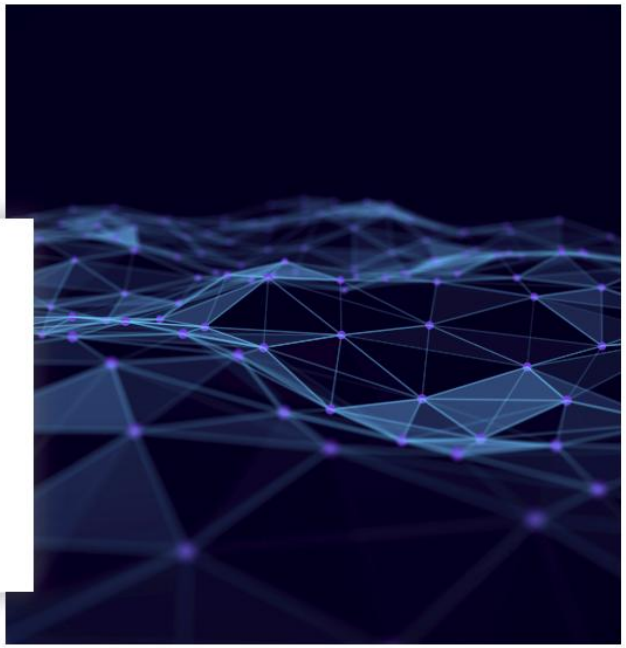
Privileged Access in Container Environment with 100,000 Servers

Global e-tailer:
Performance, scalability and flexibility for PAM in Kubernetes clusters.



Managing IT environments of 1000s of customers

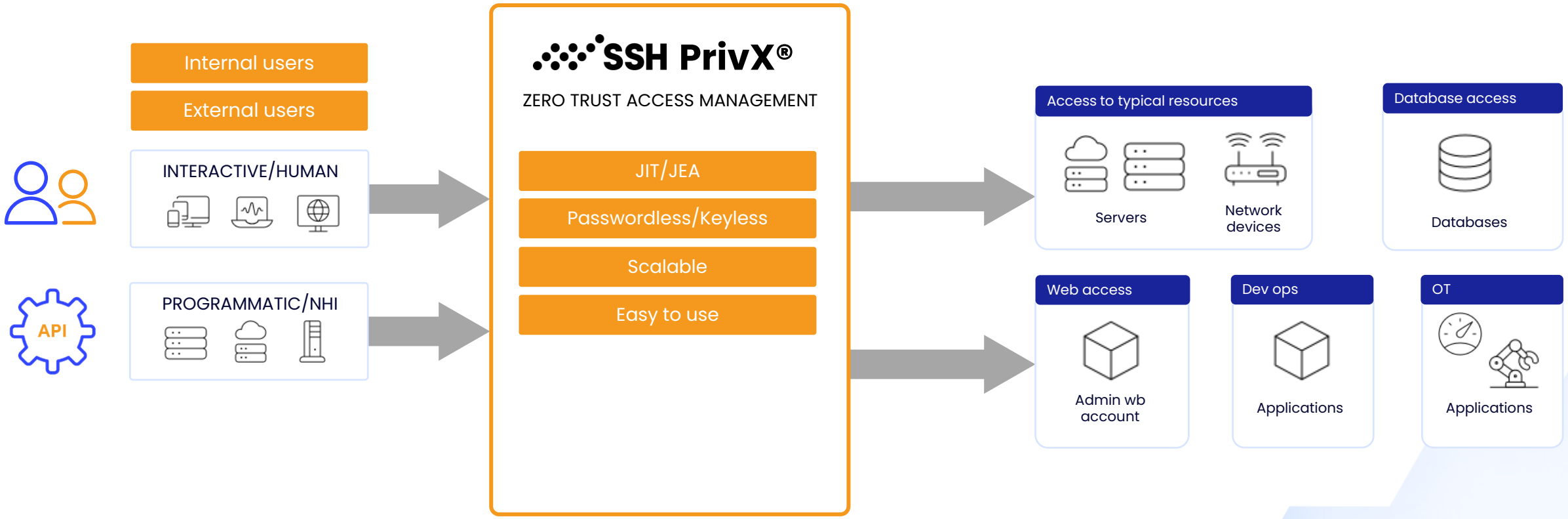
Global IT system integrator managing customer IT environments

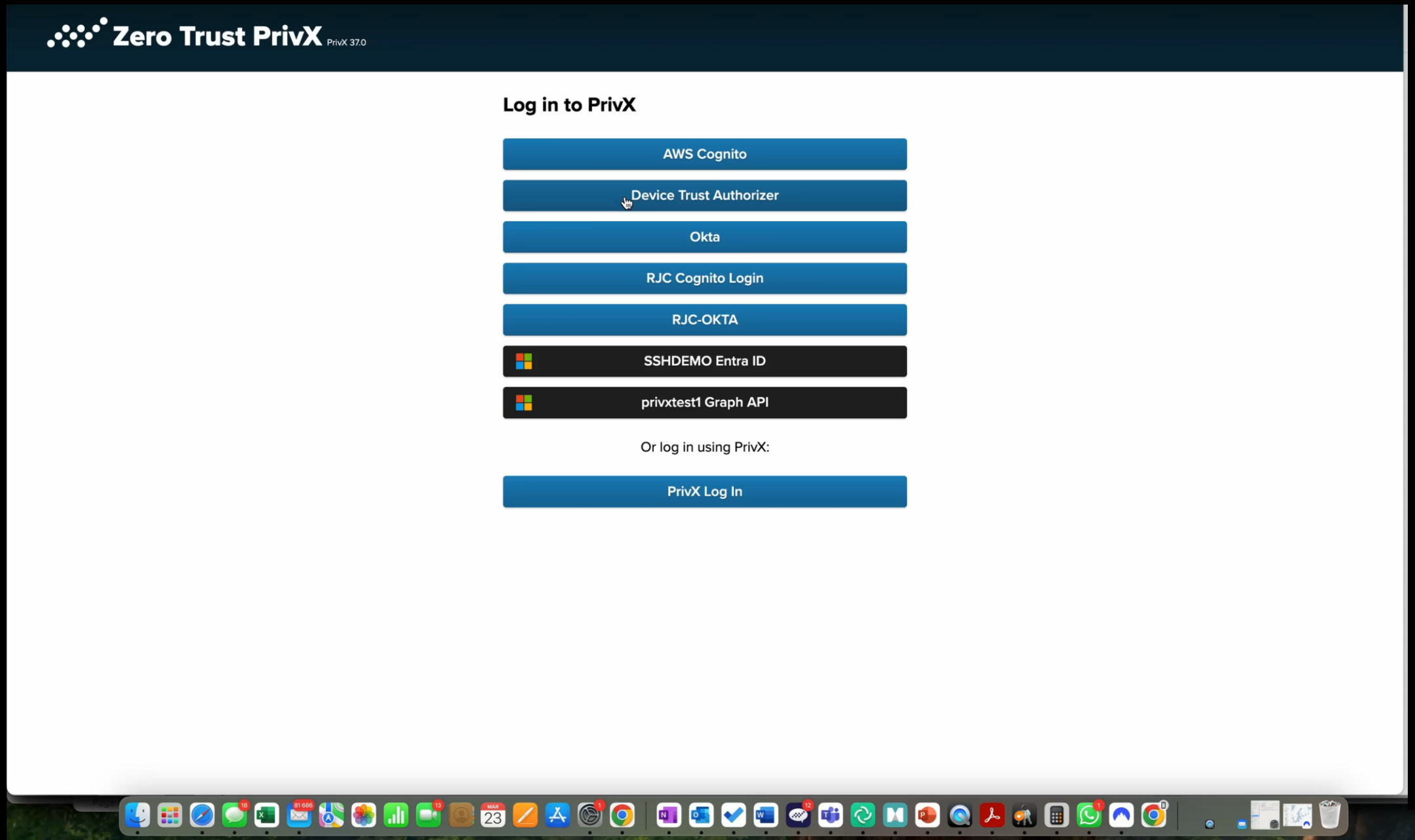


SSH

PrivX – Preventing Unauthorized Access – How does a PAM work ?

Privileged access to critical resources




Zero Trust PrivX
PrivX 37.0
Log in to PrivX
AWS Cognito
Device Trust Authorizer
Okta
RJC Cognito Login
RJC-OKTA
SSHDEMO Entra ID
privxtest1 Graph API
Or log in using PrivX:
PrivX Log In

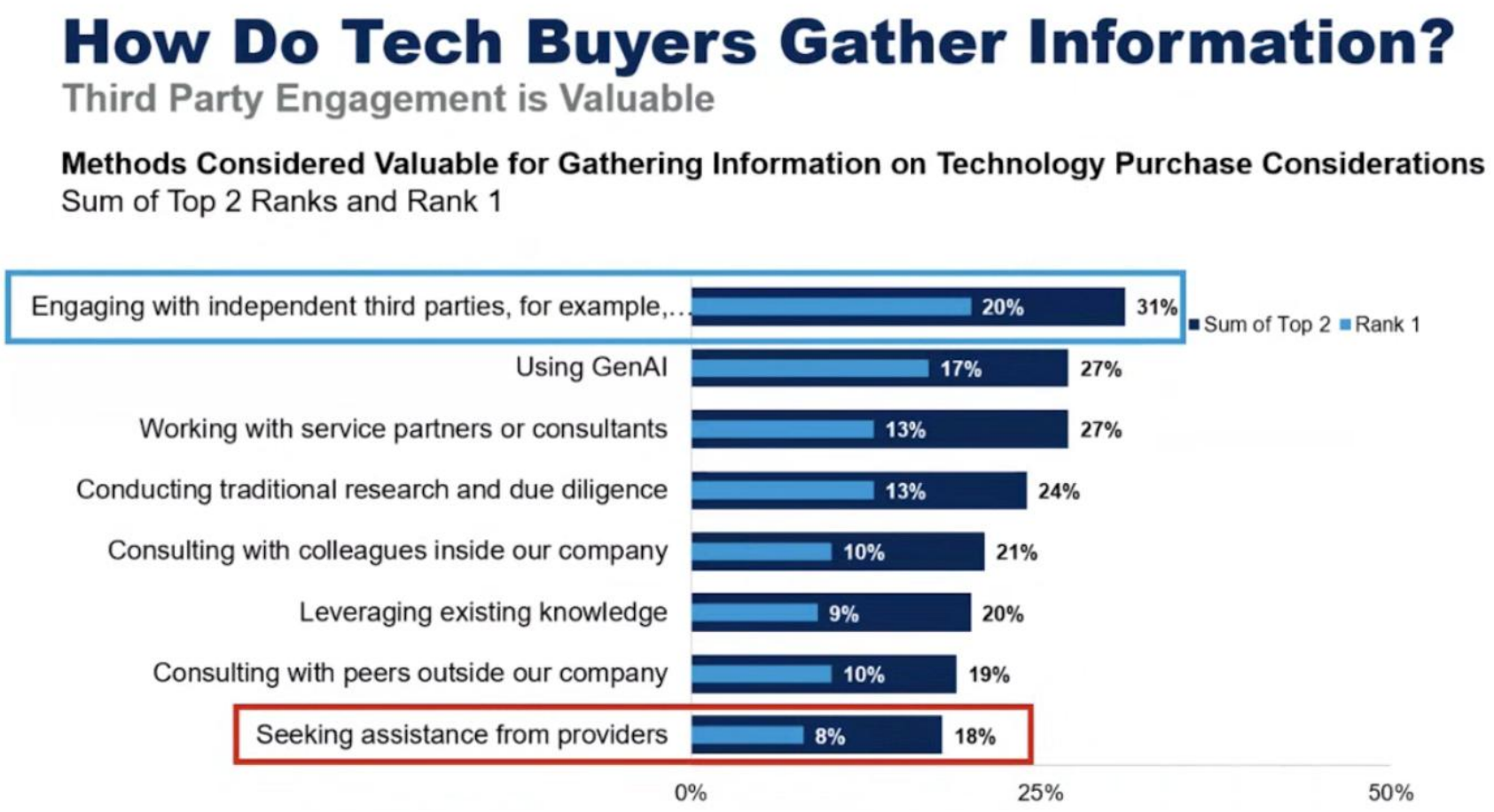
PrivX

Meets requirements

Gartner's PAM evaluation criteria:

- ☑ Privileged account life cycle management:
- ☑ Account discovery and onboarding
- ☑ Privileged credential management
- ☑ Privileged session management (PSM)
- ☑ Privileged remote access (CPS)
- ☑ Workload identity and secrets management
- ☑ Privilege elevation and delegation management (PEDM)
- ☑ Ease of deployment, maintenance and adjacent system integration
- ☑ Performance and availability
- ☑ Just in time (JIT) PAM methods
- ☑ Cloud infrastructure entitlement management (CIEM)

Why are analyst reports important ?



Gartner

SSH


NEW

Gartner®

- **“Honorable Mention” in Gartner’s Magic Quadrant for Privileged Access Management 2025.**

October 15th 2025

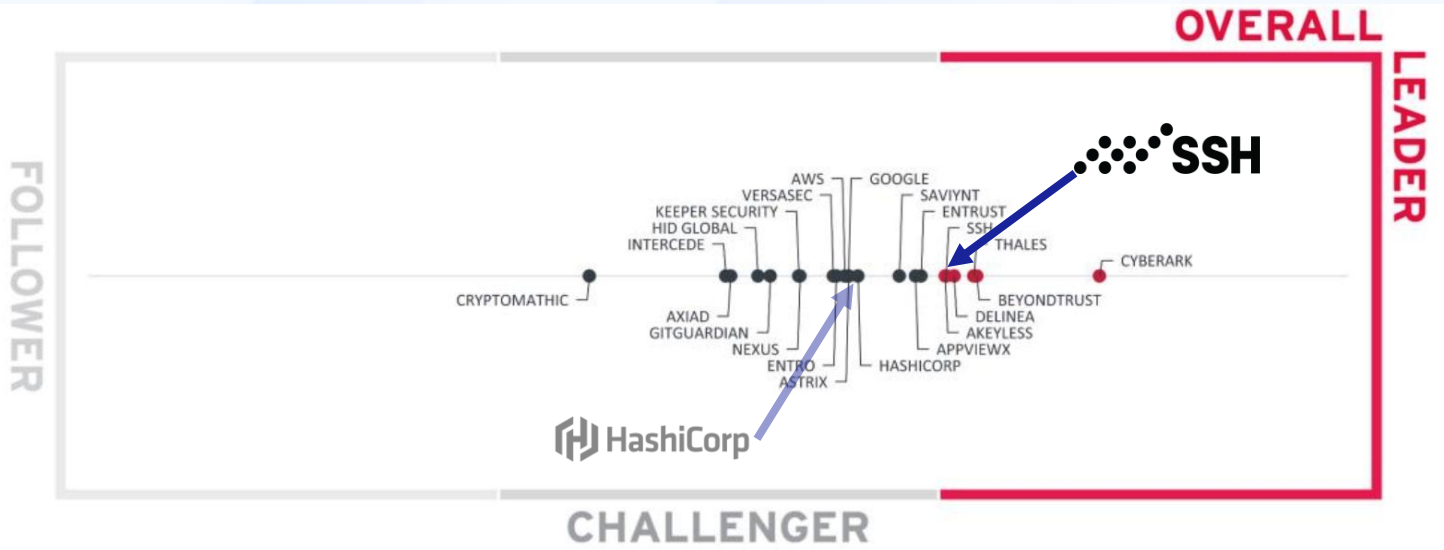
Recognized vendor in

- How to Jump-Start Your Journey Toward Passwordless Authentication
- Managing Machine Identities, Secrets, Keys and Certificates
- Leader’s Guide to Modern Machine IAM
- Voice of the Customer for Privileged Access Management

SSH

Enterprise Secrets Management Leadership Compass

kuppingercole ANALYSTS



PrivX

OVERALL LEADER | PRODUCT LEADER | INNOVATION LEADER

- Enterprise scalability with modern architecture
- Policy-based controls & leading-edge SSH key management
- Migration to passwordless and keyless access

SSH

SSH PrivX: A Modern Approach to Privileged Access Management

INFO~TECH RESEARCH GROUP

PrivX

"Overall, SSH PrivX demonstrates significant merit as a PAM solution. Its thoughtful design and alignment with zero-trust principles and zero-standing privileges make it a strong candidate for organizations aiming to enhance security without sacrificing efficiency."

-Carlos Riveira, Author of the Research

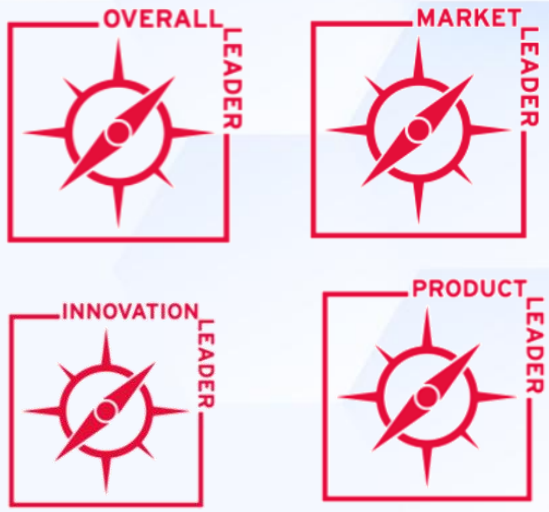
SSH

Cloud Identity and Entitlement (CIEM)Leadership Compass

kuppingercole ANALYSTS

PrivX

Leader in all categories



Decision Point for Industrial Secure Remote Access

Industrial Cyber

PrivX NQX

Innovation Grade: 4/5

Integrates secure access, PAM, and quantum-safe encryption into a unified, flexible platform with agentless OT support.

SSH

INVEST in R&D

ADJACENT POTENTIAL GROWTH DOMAINS

PrivX PAM: Adjacent Technology Domains & Potential growth markets

IAM: Identity & Access Management
IGA: Identity Governance Automation
CLM: Certificate Lifecycle Management
EKM: Enterprise Key Management (including SSH key mgmt)
WPM: Workforce Password Management
CIEM: Cloud Infrastructure Entitlements Management
CSPM: Cloud Security Posture Scanning
ZTNA: Zero Trust Network Access
SIEM: Security Information and Event Management
SOAR: Security Orchestration, Automation and Response
AV: Anti-virus
DLP: Data Loss Prevention
SWG: Secure Web Gateway
SSE: Secure Service Edge
CASB: Cloud Access Security Broker
MFA: Multifactor Authentication
ITSM: IT Service Management
SPM: Security Posture Management
HSM: Hardware Security Module

Where to Play

Trends, challenges, regulation, risks = Demand

Market segments

Solution Domains

How to Win

Solutions & **S**ervices & **S**upport

Marketing -> demand

Sales -> Partners = more feet on the ground

Voice of the customer

In-Depth Reviewer Insights

Peers Recommending This Product

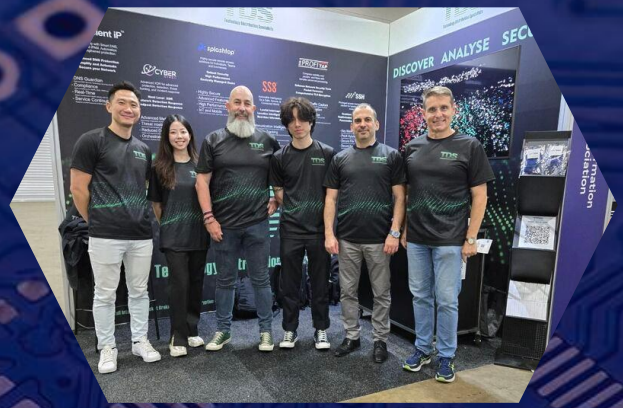
94%

Vendor	Willing to recommend	Overall rating (/5)
• SSH PrivX	94 %	4.5
• Beyondtrust	90 %	4.5
• Arcon	89 %	4.7
• Cyberark	85 %	4.4
• Delinea	87 %	4.5
• Wallix	87 %	4.5
• Oneldentity	79 %	4.2

GROW

SSH

Expand Partner business



New

宏燁資訊
ASGARD SYSTEM

accenture

COMIT

NEW

LEONARDO

Approved & Executed

SSH

- Leonardo aims to complete its extensive portfolio of space and sensors technologies to offer the most comprehensive and advanced air and missile defense system based on European technology
- Leonardo solutions are scalable and can be integrated with any kind of defense system / effector.

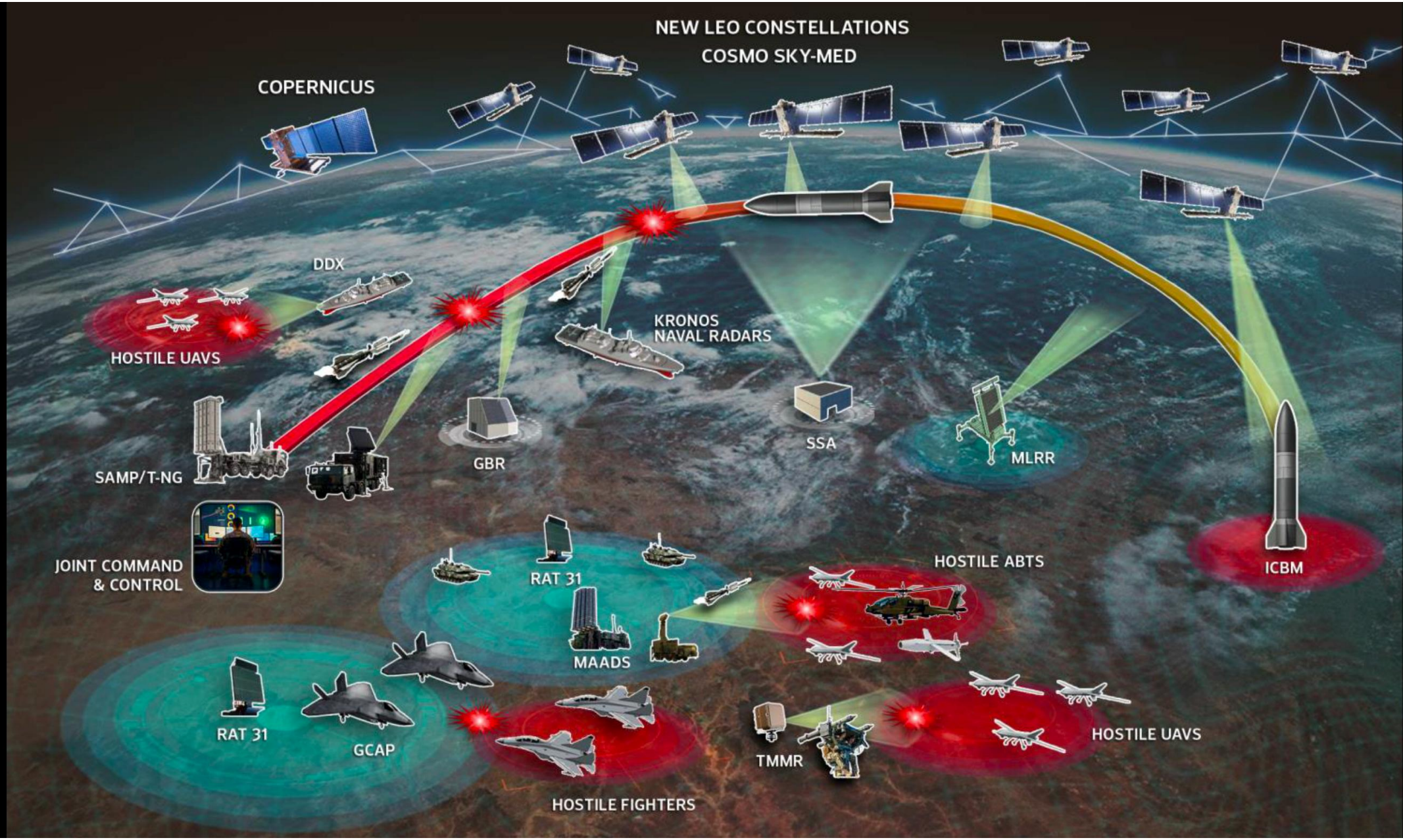
LEGENDA

TRACKING BEAM

DETECTION AREA

ENEMY DETECTED

THREAT INTERCEPT



LEONARDO

Solutions, examples

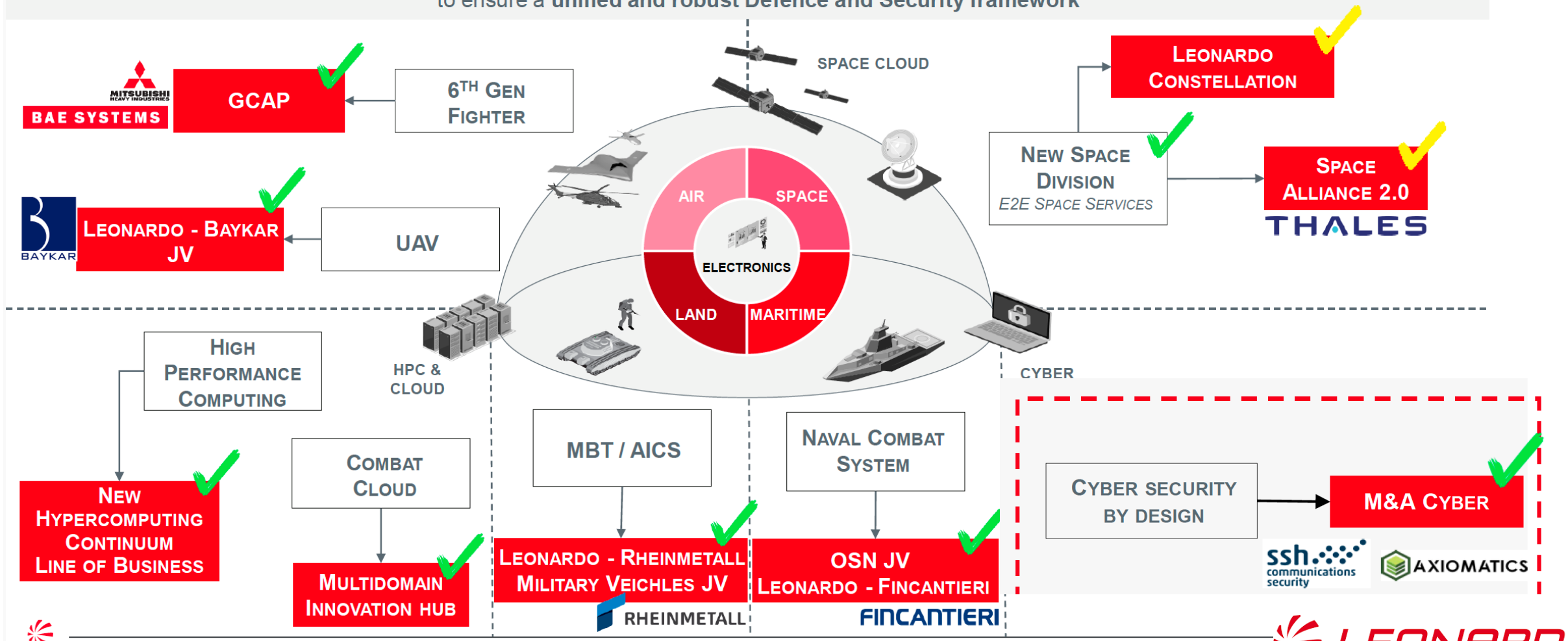
- New multi-domain Main Battle Tanks
- New Armoured Infantry Combat Systems

- UAV platforms

LEONARDO

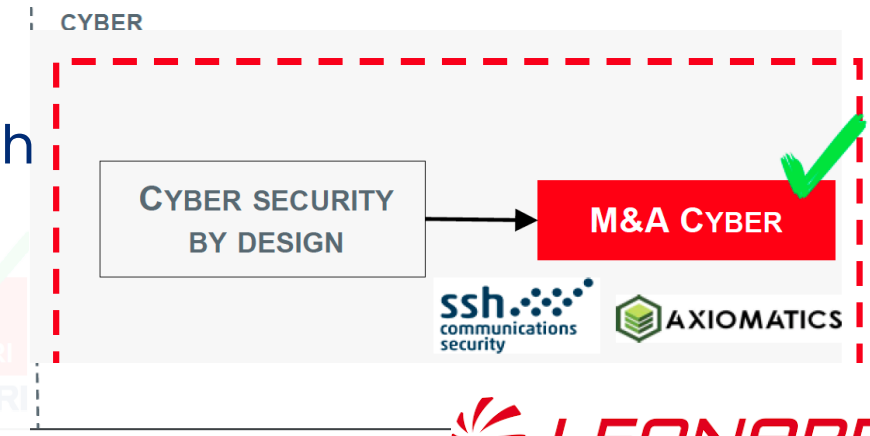
Strategic partnerships – THE Partner

Through **strategic partnerships with key players**, Leonardo is acting as the **driving force behind the Defence market consolidation**, to ensure a **unified and robust Defence and Security framework**



Strategic partnerships – THE Partner

- Cyber & Resilience Advisory, Consultancy, Services
  - GCC
  - Secure Digital & Cloud
- Complete portfolio for securing mission critical environments leveraging quantum-safe encryption
- Driving EU strategic autonomy and digital sovereignty
- Made in Europe Zero Trust revolution
- SSH's innovative cybersecurity solutions integrated with Leonardo's industrial capability and domain-specific knowledge
- HPC & AI



LEONARDO


IDENTIFY
+7%
18
Playbooks operations
DevSecOps Planned Advancements
Mean Time To Manage

GROW Sales Revenue

Growth rate 2025 has been more modest than aspired

- Decision making for projects, Investment approvals and deployment projects are taking time on customers' side
- Have made effort to turn USA business to growth, hampered somewhat with weakening USD

We are working to turn growth rate up

- Partners' onboarding and activation + Leonardo
- Increased amount of new opportunities
- Invest in Marketing & Sales
  - 2025:
    - large focus on Events – see buyers – storytelling works
    - Win Analyst endorsements and Peer recommendations
  - 2026:
    - New fresh image, content and tools
    - Improved conversion rates
    - Better SEO/AI performance
    - More traffic through campaigns and advertising

2026 and beyond

SSH

From Secure Protocols to Holistic Public Safety

SSH Communications Security Oyj

Miikka Sainio

23.10.2025

SSH

10 Years of Strategic Evolution

2016

Collection of very good standalone products

2017–2020

PrivX and Zero Trust Suite

2020

Quantum Safeness

2021

Operational Technology (OT) market focus

2025

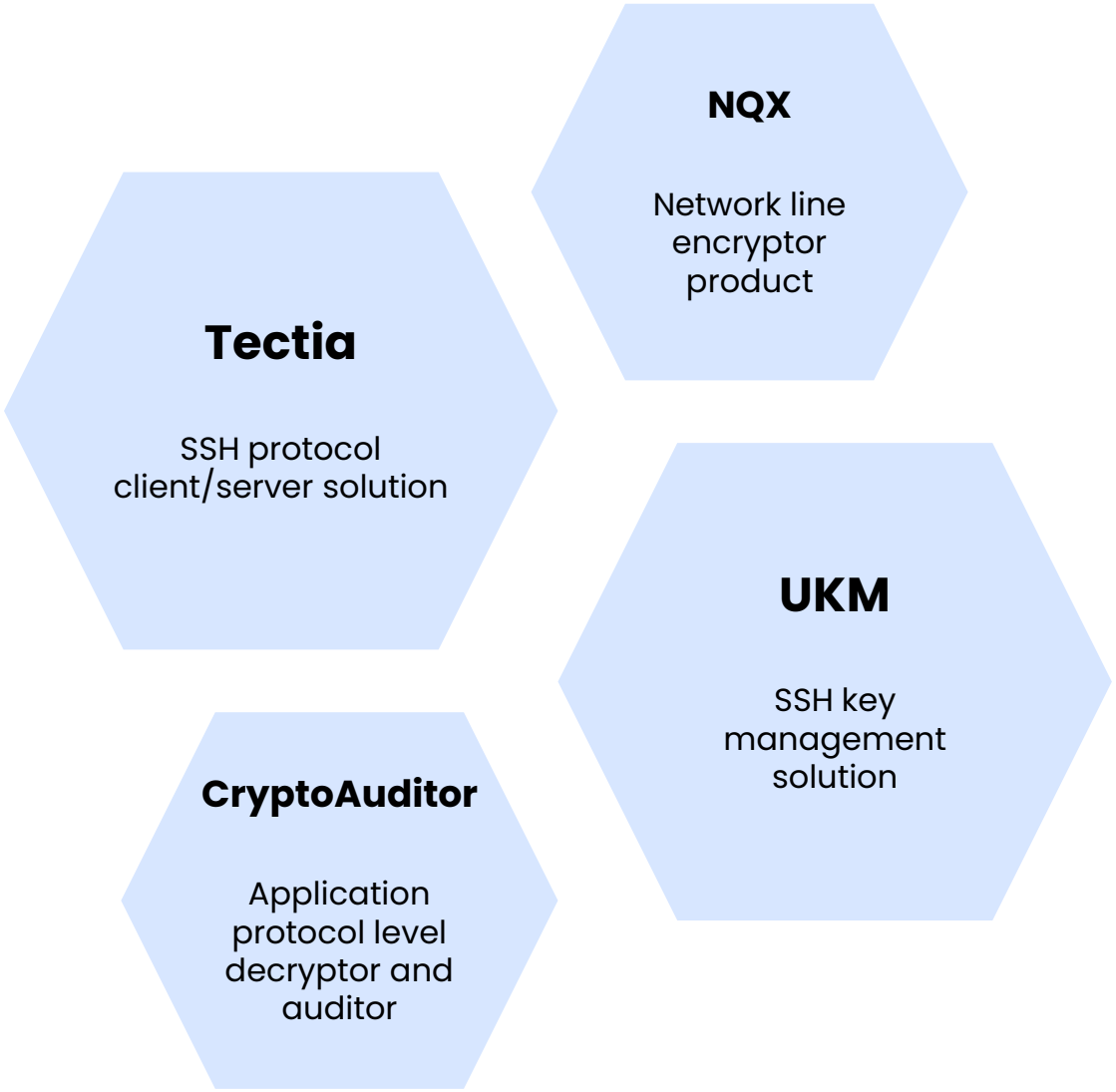
Defense sector enters the Zero Trust era

Future

AI, quantum safeness, machine identity

SSH

2016 – A Collection of Standalone Products



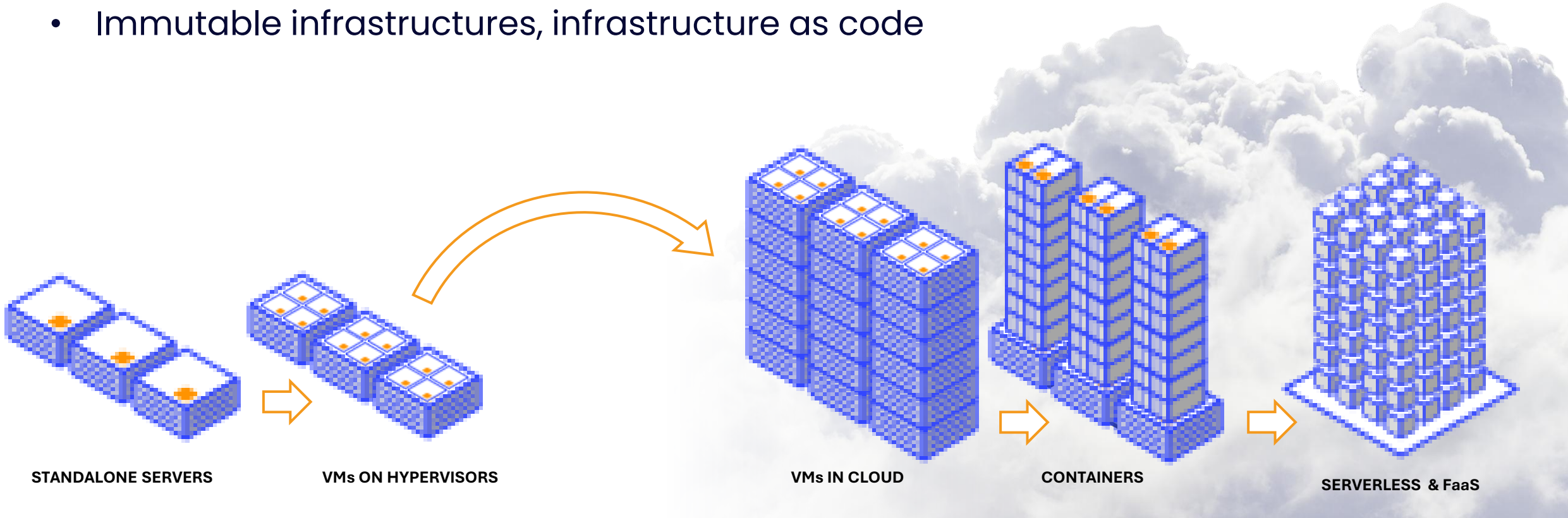
- Strong technology, fragmented portfolio
- Products sold individually with perpetual licenses
- Different technology choices, not much re-use
- Early signs that access and data security was moving toward consolidation

SSH

2017–2020: Building the Zero Trust Offering

The Computers are Evolving

- Companies strive to maximize hardware utilization
- This has led to virtualization and through that to cloudification
- Moving from “pet cow” servers to running functions in the cloud
- Immutable infrastructures, infrastructure as code



From Secure Protocols to Solutions

- SSH saw the need to move beyond the SSH protocol
- **PrivX was born** and laid the foundation for the Zero Trust suite
- PrivX provides a mechanism for just-in-time, ephemeral access
- The subscription model laid foundation for recurring revenue
- Integrable by design
- SSH became an **early mover** in Zero Trust access management

Zero Trust Adoption Timeline

2010: Forrester (Kindervag) coins Zero Trust
2011: Google publishes BeyondCorp
2017: SSH launches PrivX
2018: NIST SP 800-207 formalizes ZT Architecture
2019: Gartner coins ZTNA; UK NCSC endorses ZT
2020: CISA publishes Zero Trust Maturity Model
2021: Traditional PAM vendors reposition as Zero Trust providers
2021: US EO 14028 mandates Zero Trust in federal agencies
2022: OMB Federal ZT Strategy; EU NIS2 & DORA
2023–2025: ENISA, NATO, UK NCSC guidance and global expansion

SSH

Zero Trust Suite Creates Value

Customer value proposition

- Unified deployment, easier adoption
- Single solution to solve multiple challenges
- Policy-driven access, strong compliance support
- Scales for enterprise environments
- Manages both legacy and modern environments

Our value proposition

- Unified and shared technology stacks
- Possibility to leverage shared R&D resources
- Opportunity to **bring customers** from standalone products to solution suite

SSH

Zero Trust Suite

POST QUANTUM CRYPTOGRAPHY

ZERO TRUST

NETWORK SECURITY

OPERATIONAL TECHNOLOGY

SECURE DATA & FILE TRANSFER

SECURE COLLABORATION

SECRETS & KEY MANAGEMENT

PRIVILEGED ACCESS MANAGEMENT

Zero Trust Suite

VAULT
PASSWORD ROTATION, DEVOPS, REST API

SSH KEY MANAGEMENT

ARTIFICIAL INTELLIGENCE

VPNLESS
REMOTE PAM THROUGH BROWSER

DISCOVERY
ACCOUNTS, TARGETS

CLOUD DISCOVERY & ACCESS MGMT

LAYER2, LAYER3 ENCRYPTION

REMOTE 3rd PARTY ACCESS

PSM
PRIVILEGED SESSION MANAGEMENT

UNPARALLELED ENCRYPTION PERFORMANCE

SITE TO SITE CONNECTIVITY

OT
SECURITY & THREAT DETECTION

MESH NETWORKING

ZTNA
RBAC NETWORK ACCESS

IT
SECURITY ON-PREMISE, HYBRID- & MULTI CLOUD

DDoS RESILIENCY

PQC
QUANTUM SAFENESS & CRYPTO AGILITY

PAM
PRIVILEGED ACCESS MANAGEMENT

MFA
BIOMETRIC MFA & DEVICE TRUST

PEDM
PRIVILEGE ELEVATION & DELEGATION MGMT

AUDITING, MONITORING, UEBA

COMMAND FILTERING

FILE ENCRYPTION

SECURE EMAIL

SECURE VIDEO CONFERENCING

SECURE MESSAGING

E2E ENCRYPTION

SECURE COLLABORATION

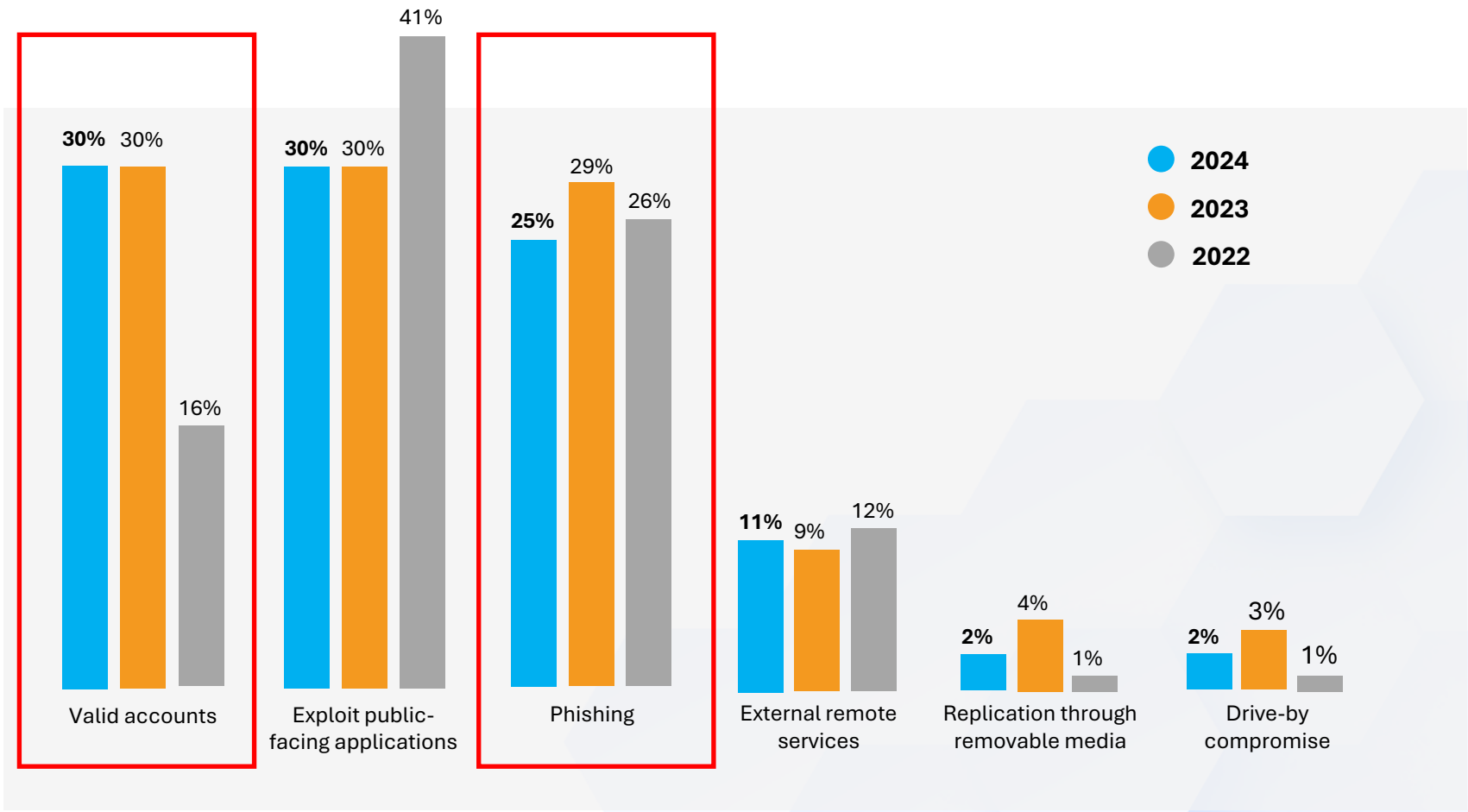
TETRA
TERRESTIAL RADIO INTEROPERABILITY

FILE TRANSFERS

Static credentials are a threat

- Shared, reused, or mismanaged passwords and SSH keys are easy targets
- SSH keys especially are problematic
- Password rotation is laborious and compute-intensive
- Stolen credentials are still the top cause of breaches

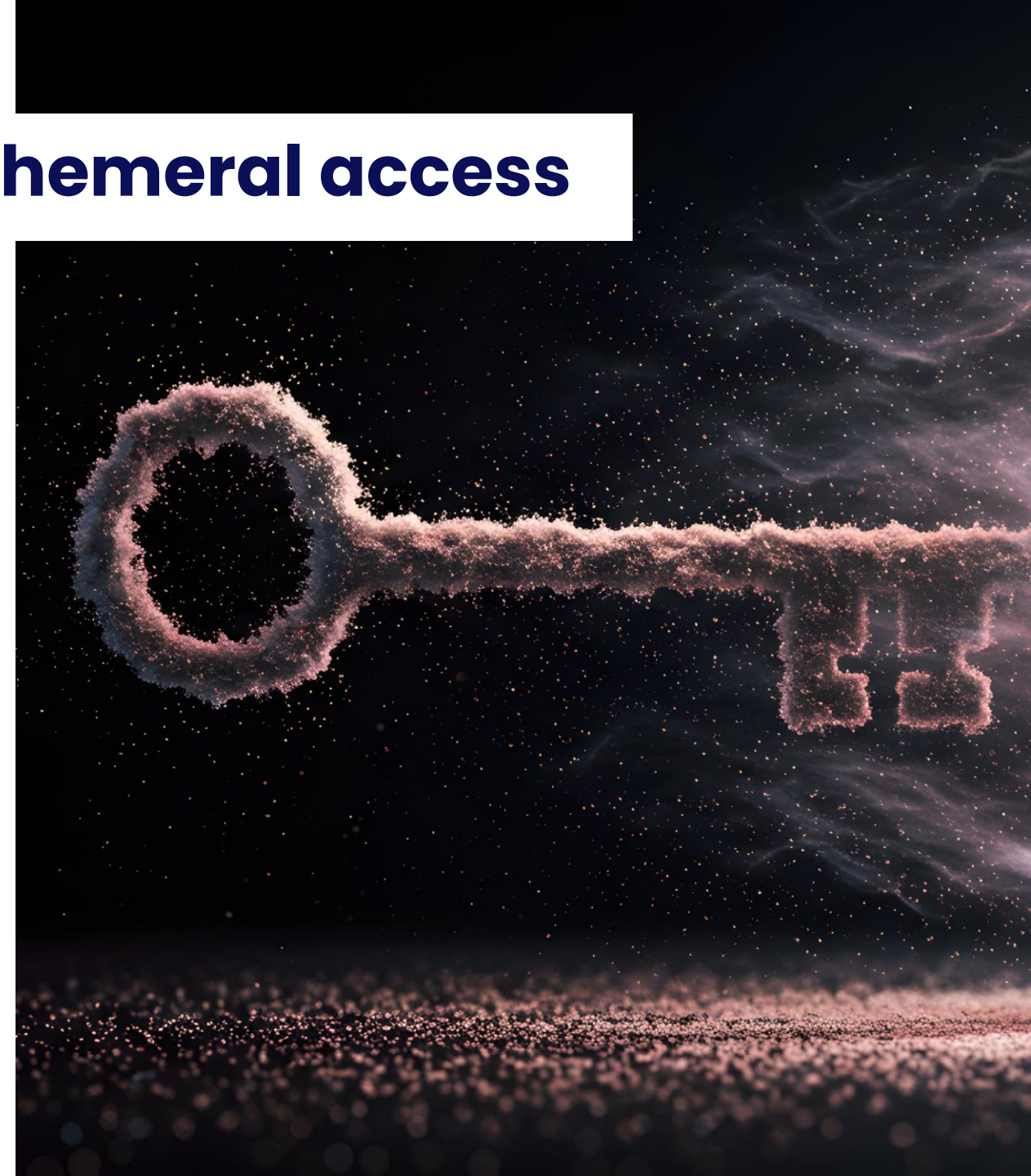
How are organizations hacked?



Source: IBM X-Force Threat Intelligence Index 2025 “Top initial access vectors in 2024 vs 2023”

Beyond passwords with ephemeral access

- Authenticate with short-lived certificates instead of stored secrets
- Identity can be verified at the time of the action
- Access is issued just-in-time and automatically expires
- Context limitations and abnormality detection routines can be imposed
- Nothing reusable, nothing to steal, **true Zero Trust**
- Extend this to the network level for Zero Trust network access - even for site-to-site connectivity



2021: From Cybersecurity to Cyber Safety

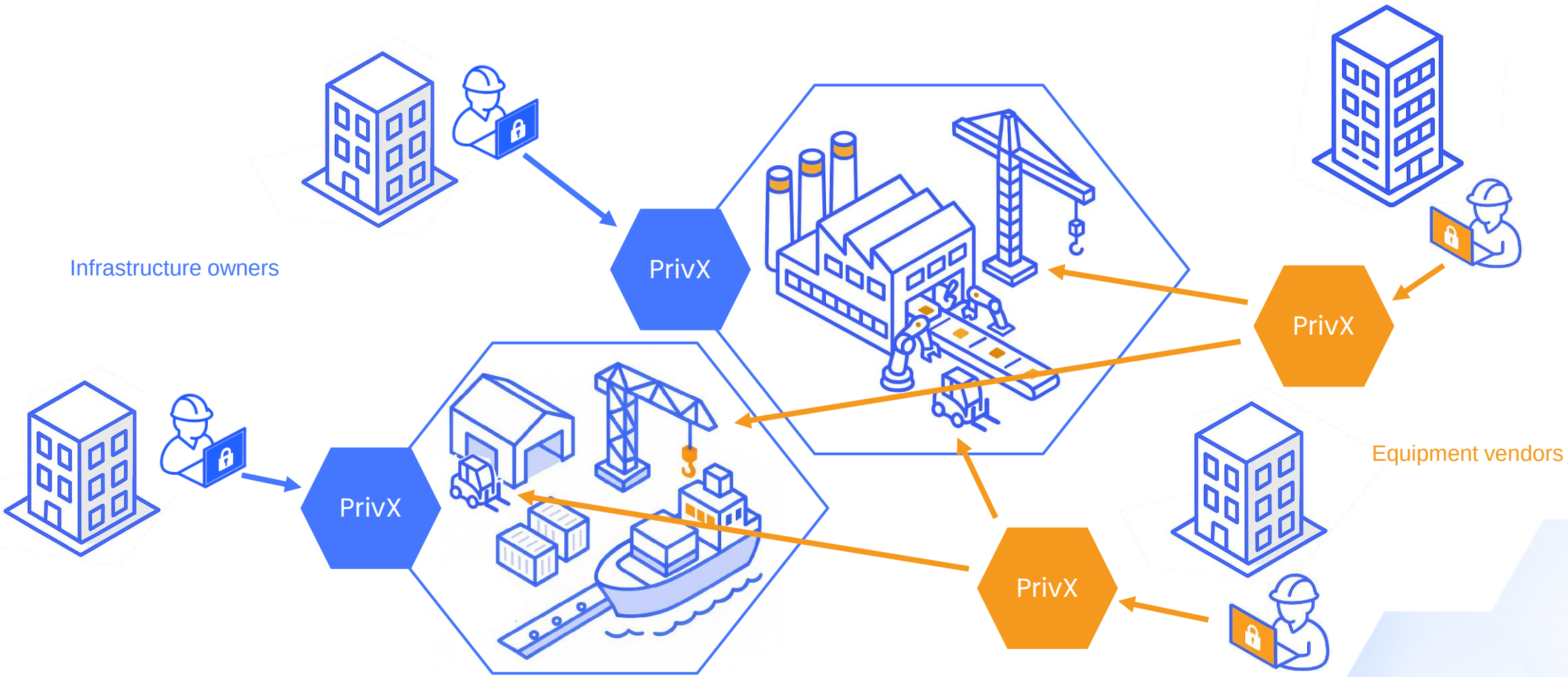
SSH

Securing Critical Infrastructure With ZT Principles

- New threat landscape: factories, energy and utilities targeted
- OT environments struggle with legacy access & compliance
- Third-party access a major pain point
- ZT solutions fit naturally: granular, identity-based access
- Significant customer adoption in industrial verticals
- Opportunity to sell to both plant or infrastructure owners and equipment vendors
- SSH became an **early mover** in OT cybersecurity

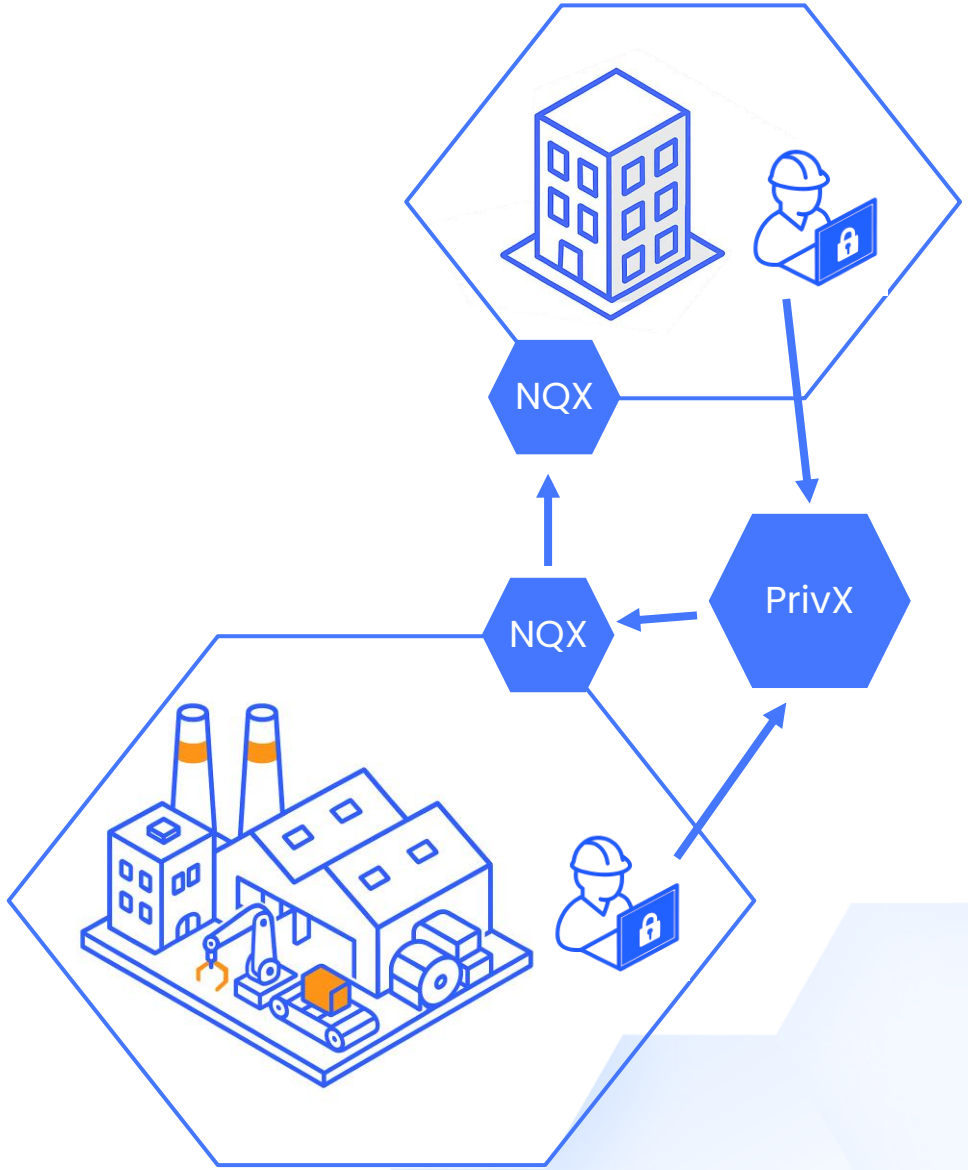
SSH

Serving Both Infrastructure Owners and Vendors

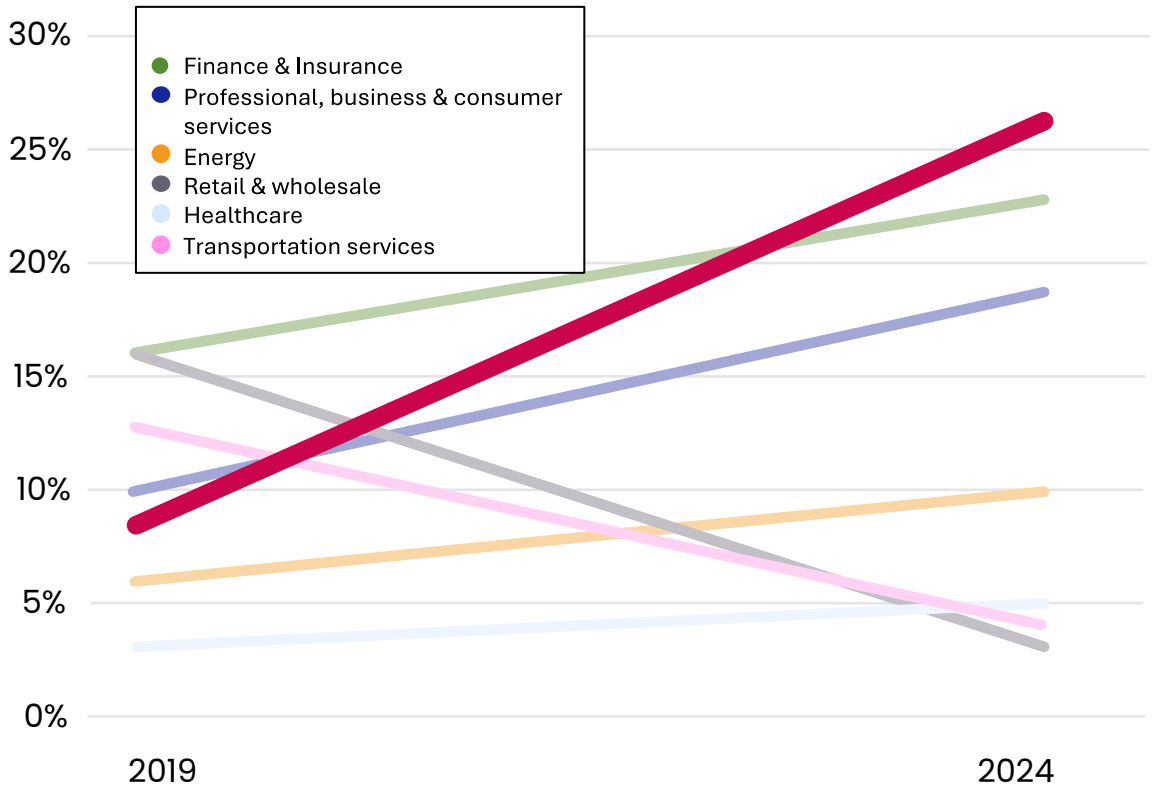


Zero Trust Network Access

- **Eliminates** always-on site-to-site tunnels
- **PrivX** provides identity verification, just-in-time session brokering & auditing
- **Site is in control** and defines the policies and approves connection
- **NQX** creates an ephemeral, identity-bound transport for the session
- **Results** in minimal attack surface, limited blast radius, and stronger OT resilience



Which Industries Are Being Attacked?



Source: IBM X-Force Threat Intelligence Index 2025

For the fourth year in a row, manufacturing is the most targeted industry

SSH

OT Security Matters – SSH Delivers It

- Critical systems can’t go down or be compromised – there are immediate real-life consequences
- Growing cyber threats – we’re seeing attackers increasingly target OT
- Regulatory pressure – governments are mandating stricter protection of critical infrastructure (EU NIS2, US CISA, IEC 62443)
- High barrier to entry and long customer relationships
- Access management solution needs to support legacy OT
- At the same time industry 4.0 is coming: connected IoT, automation, AI, …

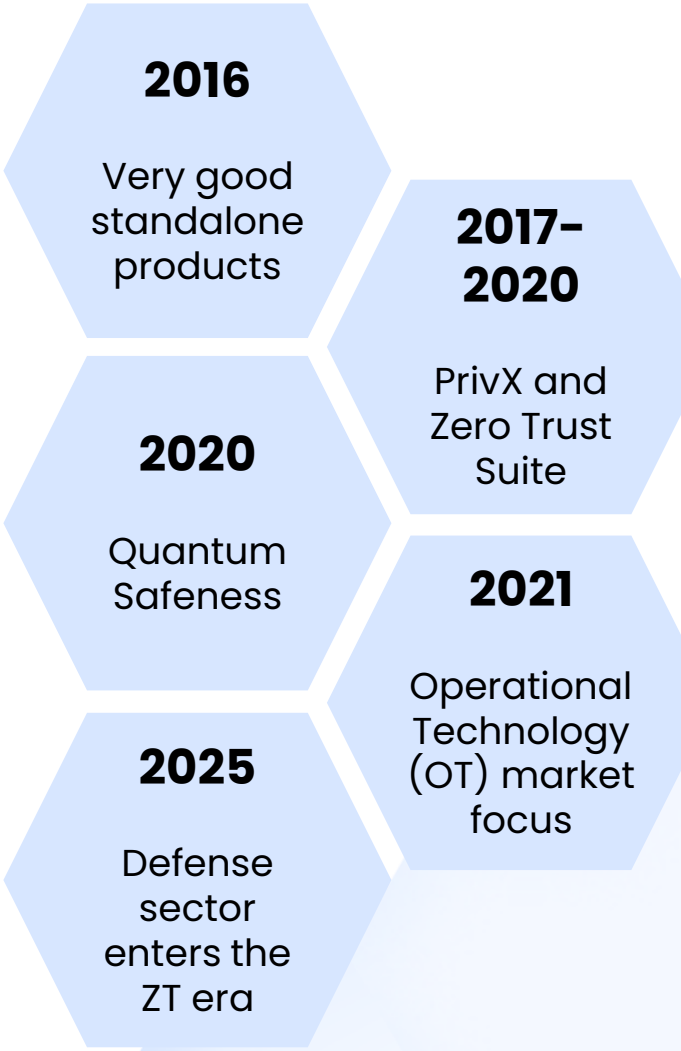
Now: SSH The Cyber Defense Company

2025 – Defense Joins the Zero Trust Era

- Geopolitical backdrop: Ukraine war & rising cyber threats
- Defense ministries in Europe and abroad accelerate Zero Trust adoption
- SSH uniquely positioned:
  - Proven Zero Trust and quantum-safe technology
  - European heritage & trust
  - Capability to operate at national security scale
- Usable, practical cybersecurity
- Zero Trust becomes a matter of **national resilience**

Strategic Significance

- We bet heavily on Zero Trust and quantum safeness
- Now we're seeing expansion from enterprise to operational technology to defense
- **Validation:** Zero Trust is not a trend, it's the future foundation in critical infrastructuree
- Defense sector adoption signals long-term demand
- SSH seen as a strategic cybersecurity partner – we have an opportunity to become an **early mover** in cyber defense



SSH

Looking Ahead – Future Horizons

- Generative AI is reshaping threats & defenses
- Quantum computing will impose the need for practical quantum safe cryptography
- Remotely securely controlling moving assets such as drones
- Through automation and agentic AI, machine identity is becoming a massive challenge

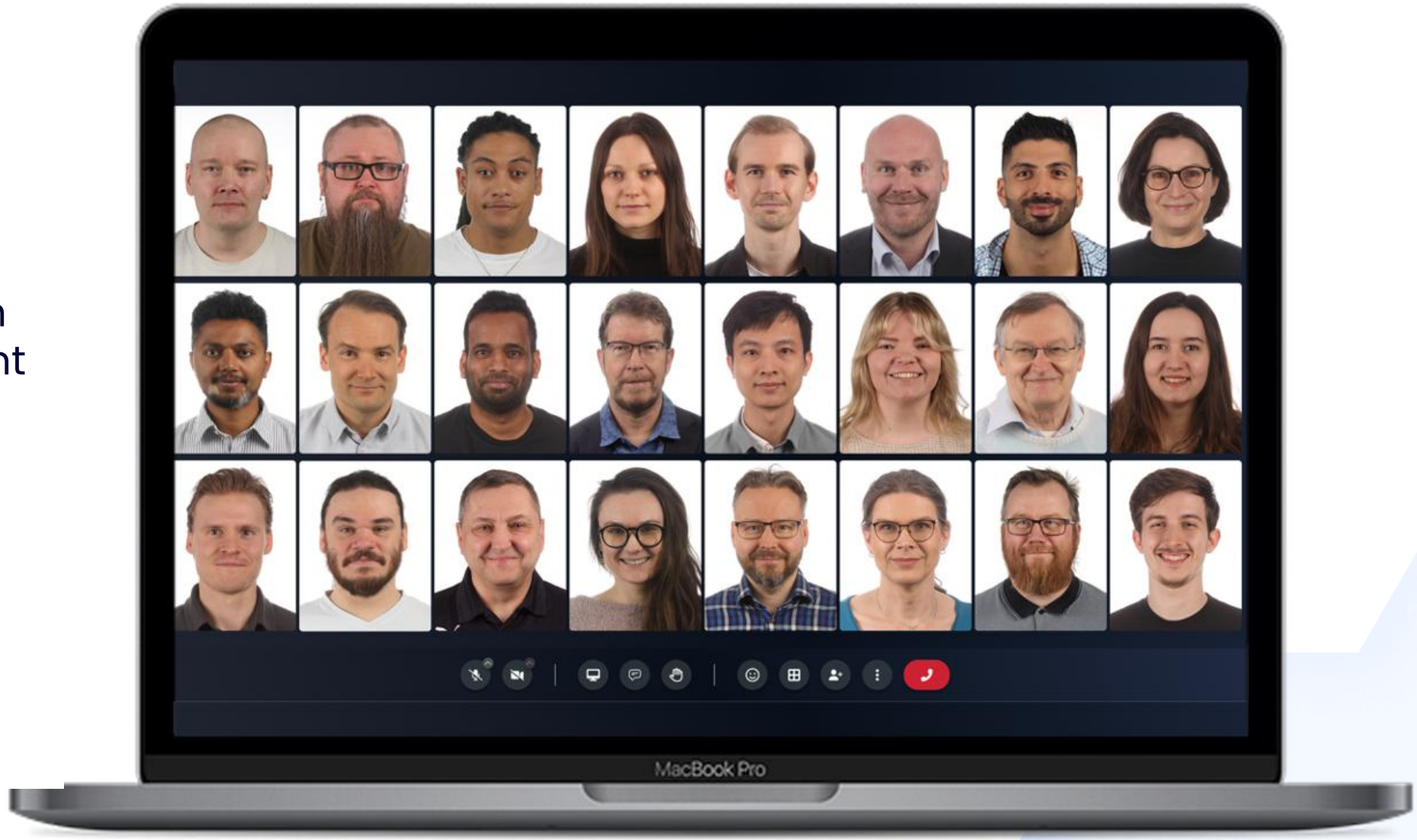
SSH is already active in all these domains.

The Team

36 nationalities

All RnD in Helsinki

No outsourcing in core development



SSH – Ready When The World Needed Us

SSH

BREAK

Integrating AI Across SSH's Operations and Solutions

Jussi Löppönen
Principal Engineer, AI

Oct, 2025

SSH

AI will be embedded in everything we do at SSH

— from internal processes to next-generation cybersecurity solutions.

Defensive Cybersecurity

Agenda

1. Present
2. Going Forward

SSH AI today

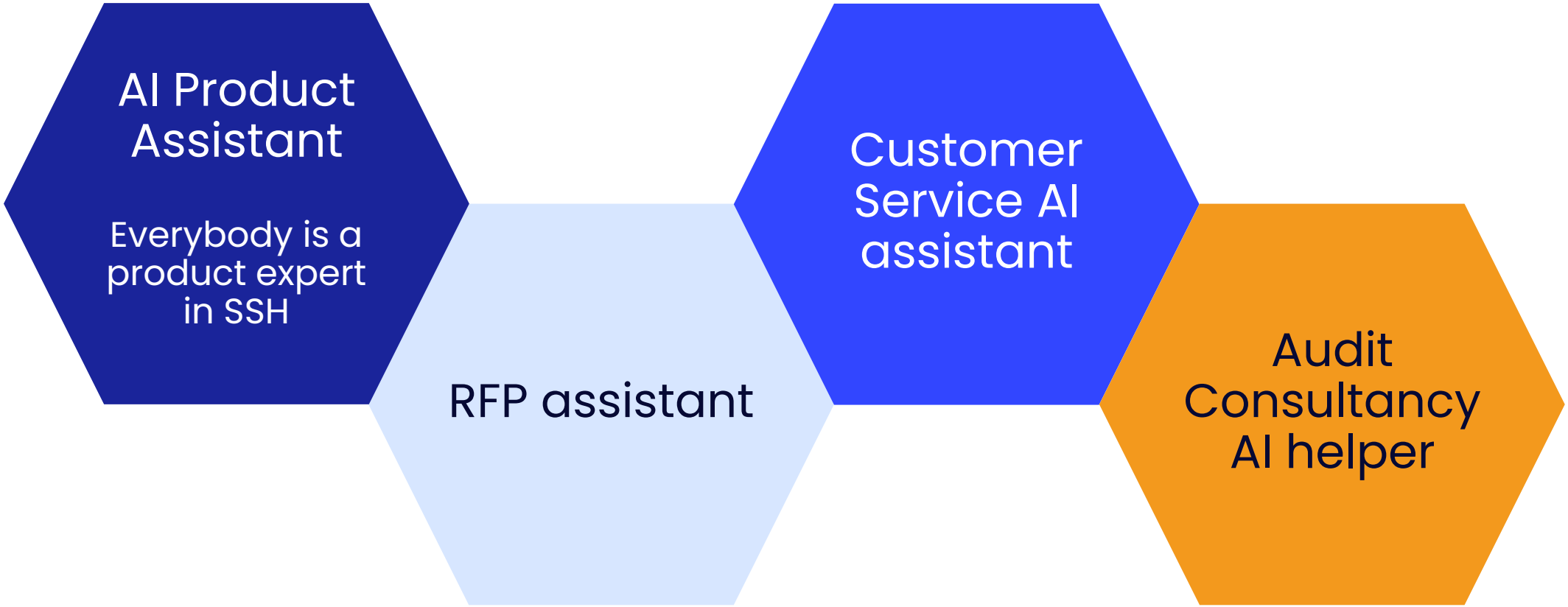
Productivity Tools

- Business process automation
- Knowledge tools
- Software Engineering tools
- Partner support tools

Customer Solutions

- PAM Anomaly Detection
- SSH key audit report

SSH Internal AI Knowledge Tools



Going Forward:
AI Cyber Security Solutions

Cybersecurity is complex environment for AI -> no over-night miracles in sight

- Security data is massive
- Correlating logs, flows, identities, and behaviors accurately is very complex challenge
  - Limited Ground Truth
  - High False Positives
- Cost
  - More intelligence -> more expensive

➢ AI often remains at advisory level, not real-time defense

SSH

AI-driven Innovation adopted in SSH expands possibilities to address the complexities

— setting the stage for new offerings in 2026

AI has transformed business development

Real-time BI insights and competitive intelligence

Accelerated innovation with synthetic data, AI data analysis and rapid prototyping

Faster system design, coding, and testing through AI

SSH's cybersecurity AI model is in our toolbox

- Data-secure AI solutions with edge deployment options
- We invested into research during 2025
  - Down streaming an open source LLM to cybersecurity domain
  - Science and available technologies enable this
- Scoring and benchmarking show consistent, promising results across evaluation sets
- We are evaluating the business possibilities

Direction for SSH Cybersecurity AI Solutions

- We have an AI-powered innovation and R&D process underway, targeting a 2026 launch
- AI will broaden our cybersecurity capabilities beyond privileged access helping to protect our customer IT systems e.g. in large banks
- More news to follow 2026

AI will be embedded in everything we do at SSH

— from internal processes to next-generation cybersecurity solutions.

Defensive Cybersecurity

Quantum-safe era is here

Suvi Lampila, SSH Fellow

SSH

Post-Quantum Cryptography transition does not need or wait for advances in quantum technology itself.

Recommendations and legislation come into effect

POLICY AND LEGISLATION | Publication 23 June 2025

A Coordinated Implementation Roadmap for the Transition to Post-Quantum Cryptography

The EU Member States, supported by the Commission, issued a roadmap and timeline to start using a more complex form of cybersecurity, the so-called post-quantum cryptography (PQC).

H.R.7535 - Quantum Computing Cybersecurity Preparedness Act

117th Congress (2021-2022)

LAW Hide Overview ✕

Sponsor: Rep. Khanna, Ro [D-CA-17] (Introduced 04/18/2022)

Committees: House - Oversight and Reform | Senate - Homeland Security and Governmental Affairs

Latest Action: 12/21/2022 Became Public Law No: 117-260. (All Actions)

Roll Call Votes: There has been 1 roll call vote

Tracker: Introduced > Passed House > Passed Senate > Resolving Differences > To President > **Became Law**

Monetary Authority of Singapore

10 Shenton Way MAS Building Singapore 079117
Telephone: (65) 6225-5577

Circular No. MAS/TCRS/2024/01

20 February 2024

To Chief Executive Officers of All Financial Institutions

Dear Sir / Madam

ADVISORY ON ADDRESSING THE CYBERSECURITY RISKS ASSOCIATED WITH QUANTUM

Quantum computers that harness the laws of quantum mechanics have the potential to solve certain mathematical problems exponentially faster than traditional computers to bring substantive transformation to a diverse range of industries. At the same time, their potential to break some of the commonly used encryption and digital signature algorithms poses a major cybersecurity concern. The security of financial transactions and sensitive data that financial institutions ("FIs") process could be at risk with the advent of these cryptographically relevant quantum computers ("CRQCs")[1].

Full transition requires industry-wide effort globally

BEYOND THE LIMITS OF POST-QUANTUM CRYPTOGRAPHY

Beyond the Limits of PQC
UNIVERSITY OF HELSINKI
UNIVERSITY OF OULU
Aalto University
SSH
Bittium
ERICSSON
VTT
CIPHERA
JUTEL
icareus
TRAFICOM
DIGI- JA VÄESTÖTIETOVIRASTO
Puolustusvoimat
The Finnish Defence Forces

SSH

We can defend the data with Quantum-Safe encryption only in advance.

Transition to Quantum-Safe Confidentiality is on-going but only the first step

Adoption of Post-Quantum key exchange for web traffic.

43%
Finland
<30% Oct 2024

35%
World-wide
20% Oct 2024

29%
US
<20% Oct 2024

Cloudflare Radar October 2024-2025

SSH

Affected Security Applications

Virtual Private Networks (VPN)

Transport Layer Security (TLS)

Secure Shell (SSH)

Secure Email

Instant messaging

User Authentication

Digitally signed documents

Blockchain transactions

Quantum-Safe Authentication is needed next

Many credentials need to be discovered and re-issued before Day One of Cryptographically Relevant Quantum Computer

Privileged

Access and Signing Credentials

Human

Access Credentials, IDs and Credit Cards

Machine

Public-key based authentication

Certification Authorities

Trusted for firmware signing, financial and legal transactions

SSH

SSH solutions are already defending Quantum-Safe world

SSH

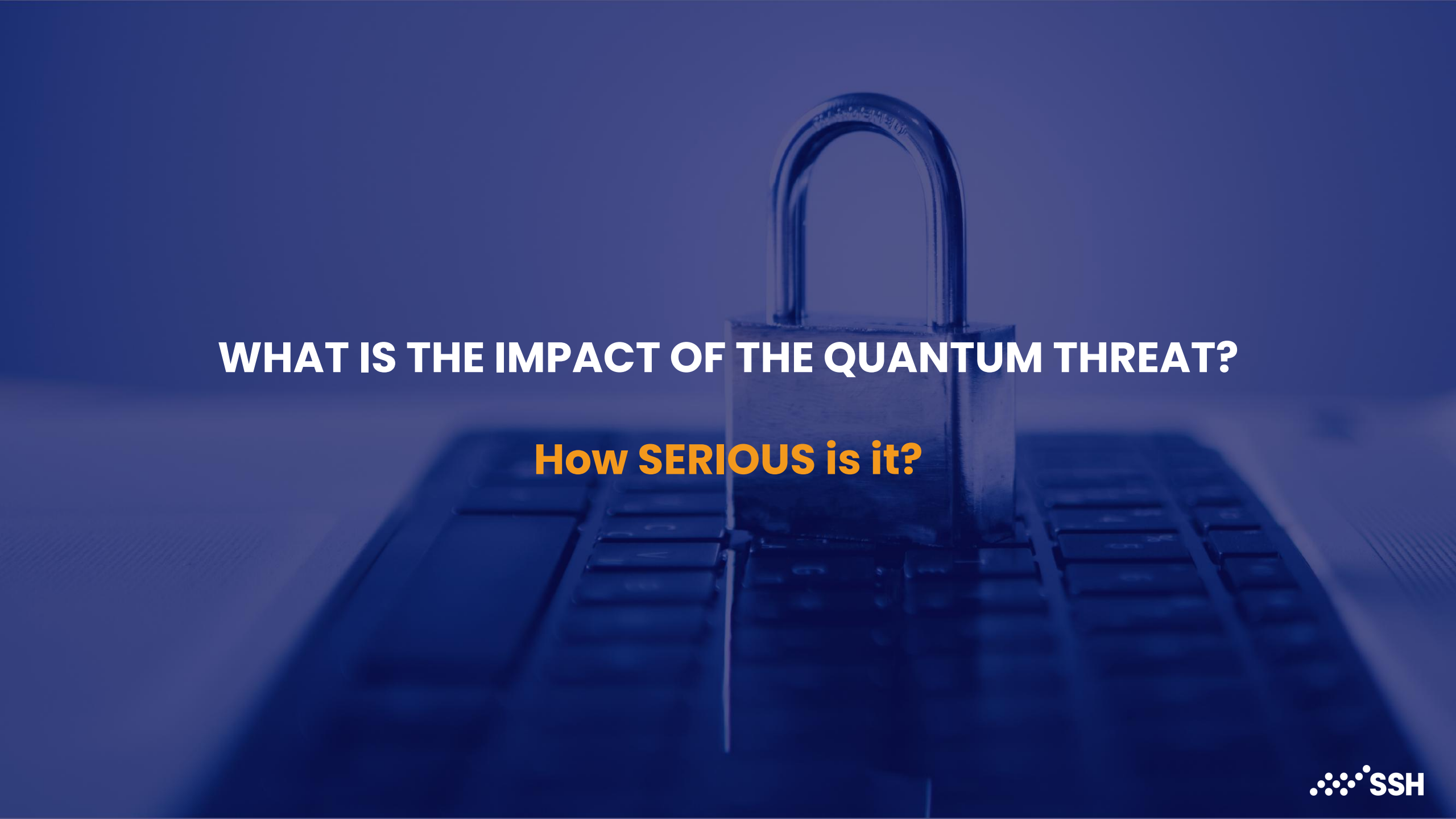
Quantum-Safe Discussion

Tero Mononen *Principal Engineer*
Suvi Lampila *SSH Fellow*
Rami Raulas *CEO*

SSH

WHAT IS THE QUANTUM THREAT AND RISK?

SSH



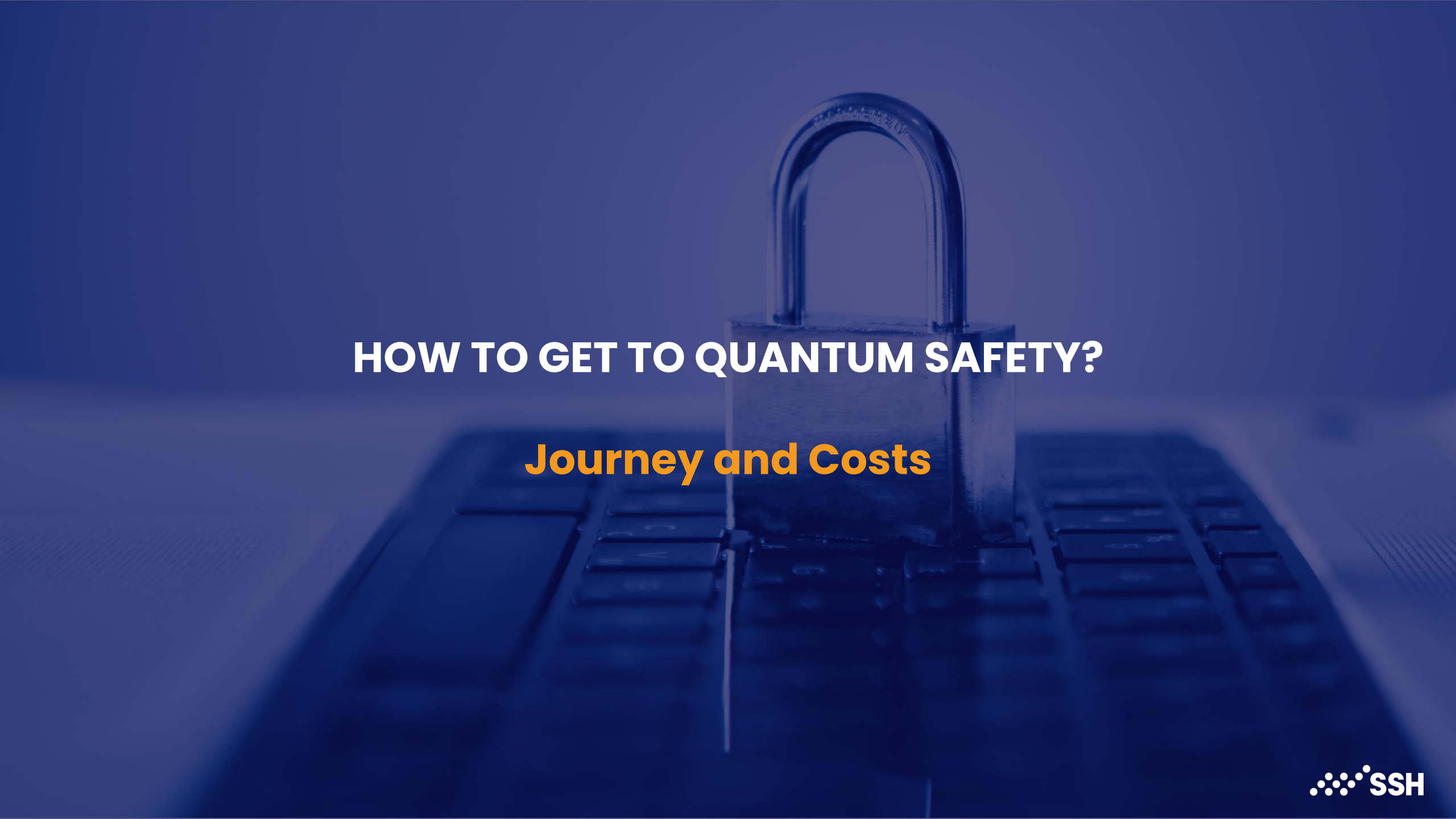
WHAT IS THE IMPACT OF THE QUANTUM THREAT?

How SERIOUS is it?

SSH

HOW TO MITIGATE THE QUANTUM THREAT?

SSH



HOW TO GET TO QUANTUM SAFETY?

Journey and Costs

SSH

- The quantum threat is REAL and manageable in steps
- PQC (Quantum-Safe) transition is already ongoing and will happen broadly
- Regulation (e. g. EU CER/CRA/NIS2/ENISA) mandates
  - Zero Trust in critical infrastructures
  - Secure Products with Quantum-Safe encryption
- Quantum-Safe is business enabler for SSH

SSH

Leonardo and SSH

Simone Ungaro,
Co-General Manager, Strategy & Innovation

LEONARDO

SSH

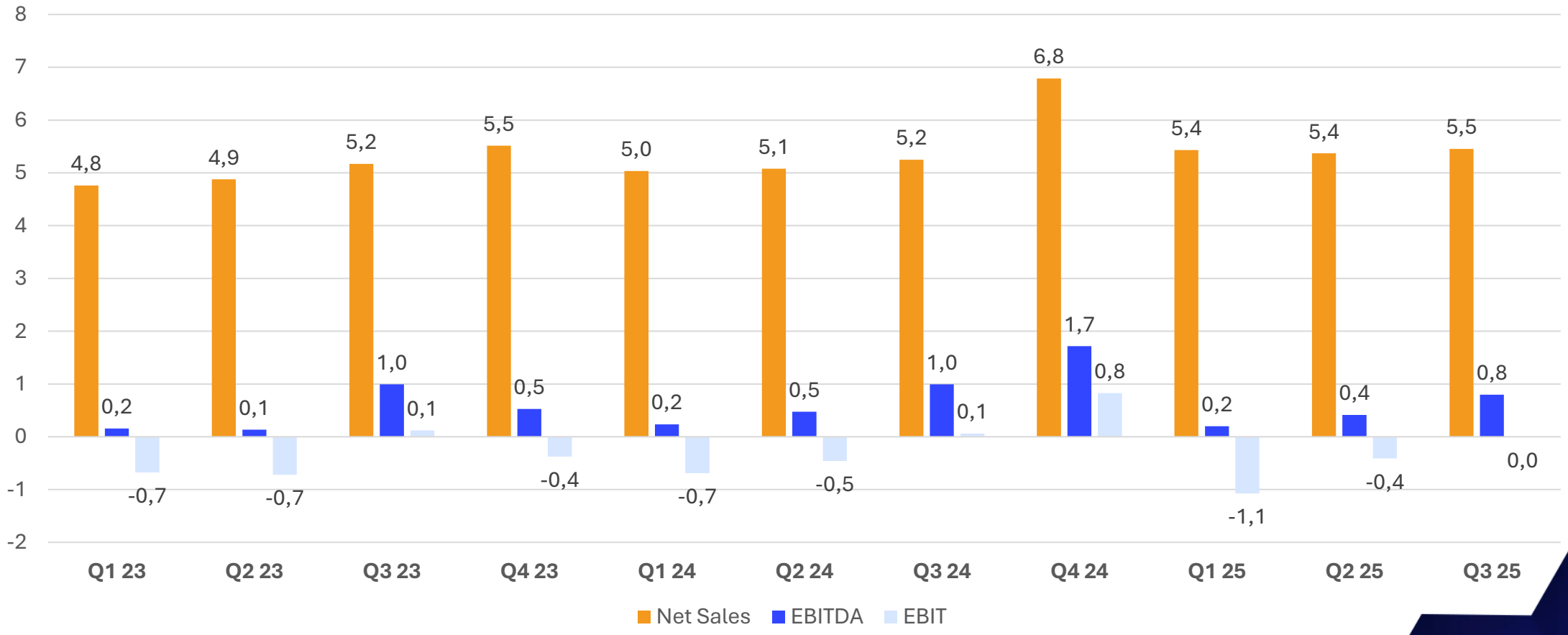
Financial update

Michael Kommonen, CFO

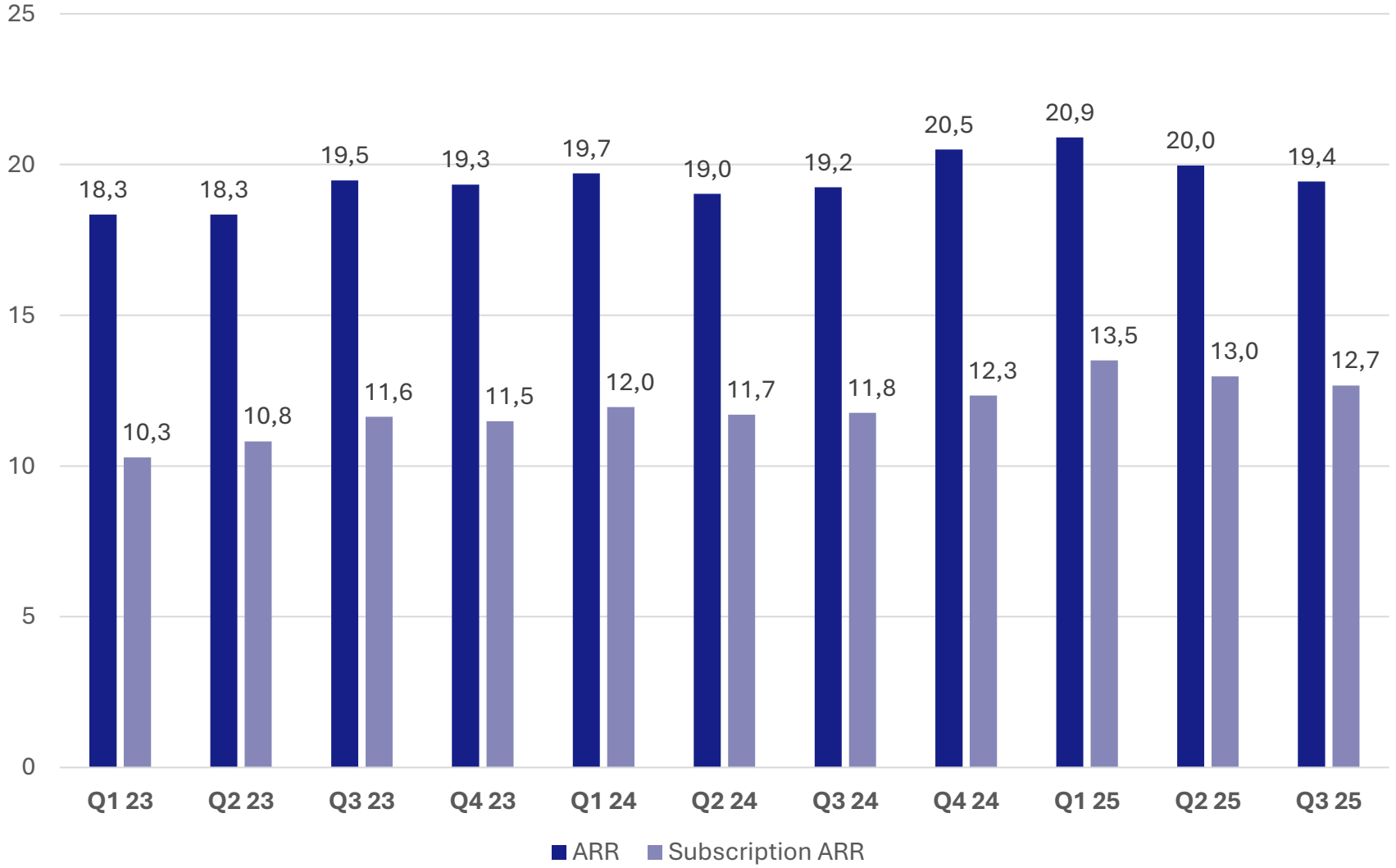
Leonardo transaction update

- Deal was announced **1 July 2025**
- 20 mEUR directed share issue and strategic partnership agreement
- Subject to approval by Finnish Ministry of Economic Affairs and Employment Foreign Direct Investment regulation
- Deal closed on **21 October 2025** after a regulatory review period that was slightly longer than anticipated
- Leonardo S.p.A. appointed Francesco Di Sandro, SVP Strategy – Cyber & Security Solutions Division

Net Sales, EBITDA, EBIT

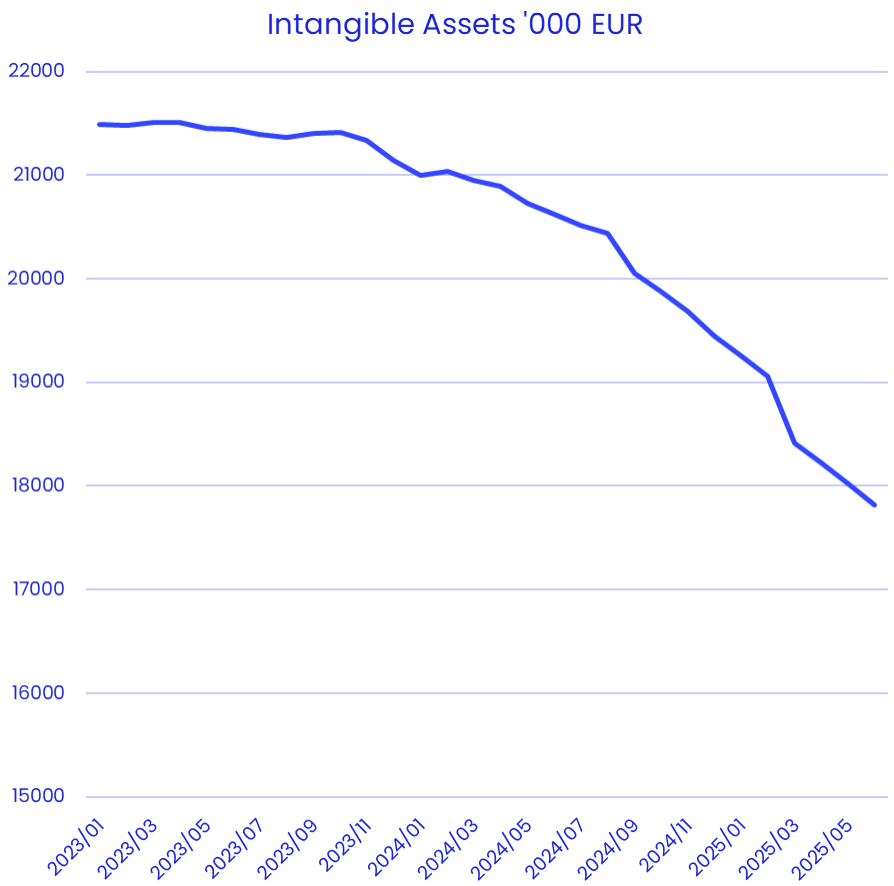


Recurring revenue



- Seasonal decline in ARR in Q3 2025 due to delays in certain contract renewals where expansions are being negotiated

Change in accounting of R&D cost expenditure



- Balance sheet lightened since end of 2023
- Reducing intangible assets over time
- R&D expense increasingly booked as cost vs investment -> D&A outpacing activations
- Has in short term burdened EBITDA development
- Longer term will reduce depreciations and amortizations and reduce gap between EBITDA and EBIT

Accelerating growth with proceeds from share issue

Strengthening R&D organization with emphasis on further improving PrivX competitive position on the PAM market

Increasing Sales & Marketing resources globally

Simplifying balance sheet through reduction of hybrid loan

SSH market offering and partnerships positioning for growth

- Sales growth to accelerate in 2026 and beyond, driven by Leonardo partnership
- Annual sales growth will fluctuate somewhat depending on subscription-license sales mix

- EBITDA and cash flow from operations expected to be positive in 2026 and improve further in 2027

Q&A

SSH

Global & EMEA Headquarters
SSH Communications Security Oy
Karvaamokuja 2D
00380 Helsinki
Finland
Tel. +358 20 500 7000
info.fi@ssh.com

AMER Headquarters
SSH Communications Security Inc.
66 Hudson Blvd E, Suite 2308
New York, NY, 10001
USA
Tel. +1 (212) 319 3191
info.us@ssh.com

APAC Headquarters
SSH Communication Security APAC
6 Raffles Boulevard, Marina Square, #03-308
Singapore, 039594
Singapore
Tel. +65 6338 7160
apac.sales@ssh.com